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

UNIVERSITÉ SAAD DAHLAB BLIDA

FACULTÉ DES SCIENCES

Mémoire de fin d'étude
Pour l'obtention d'un diplôme de Master en Informatique
Option : Sécurité des Systèmes Informatiques

Conception et réalisation d'une application de gestion des Accès logiques des utilisateurs Privilégiés

Organisme d'accueil : ELIT (El Djazair Information Technologie)

Réaliser Par :

- Amri Fouad
- Akour Karim

Encadré Par :

- Mme Zahra fatma Zohra
- Mr Sayad Saad

Jury :

- Mme. Aroussi sana	Président
- Mme. Arkam Meriem	Examinateur
- Mme Zahra fatma Zohra	Promoteur
- Mr Sayad Saad	Encadreur

Promotion :2017/2018
Date de soutenance : 27/09/2018

Remerciements

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 Zahra Fatma Zohra, Nous la remercions de nous avoir encadré, orienté, aidé et conseillé.

Nous tenons à remercier vivement notre maitre de stage, Mr Sayad Saad, Chargé de la division DataCenter TAKA au sein de l'entreprise ELIT, 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 Madame Sahad Imane Directrice du la direction exploitation des systèmes d'information et toute l'équipe pour leur accueil, leur esprit d'équipe et en particulier Mr Toufik.

Madame Arroussi sana président du jury, et Madame Arkam qui ont accepté de nous consacrer leurs temps en examinant le mémoire. Nous sommes honorés et on leur exprime toute 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 ».

Madame Rezoug, Vous êtes le professeur qui a réussi à nous inspirer, à nous donner confiance en soi et en l'avenir mais aussi qui a réussi à nous donner l'envie d'apprendre. Merci pour tout ce que vous avez fait.

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

Table des matières :

Table des figures

RESUME

Notre projet se concentre sur l'étude, la conception et réalisation d'un outil de gestion des accès privilégiées pour la société ELIT « EL Djazair Information Technology », afin d'augmenté le niveau de sécurité de son système d'information et enrichir de plus en plus ces moyens de parade contre les dangers de cyber criminalité et les employés mécontent.

Les objectifs majeurs de ce projet sont le contrôle d'accès aux ressources critiques de leur DATA CENTER et la traçabilité totale des utilisateurs privilégiés.

ABSTRACT

Our project focuses on the study, design and implementation of a privileged access management tool for the Company ELIT "EL Djazair Information Technology", in order to increase the security level of its information system and enrich more, and increase defense mechanism against the dangers of cybercrime and employees dissatisfied.

The main objectives of this project are the access control to the critical resources of their DATA CENTER and the total traceability of the privileged users.

ملخص

يركز مشروعنا على دراسة وتصميم وتنفيذ آلية لإدارة ولوج المستخدمين ذوي الإمتييازات لشركة الجزائر أنفورماسيون تكنولوجي ، من أجل زيادة مستوى الأمن في نظام المعلومات الخاص بها وإثراءه بلمزيد من الآليات لمواجهة مخاطر الجريمة السيبرانية والموظفين غير راضين

تتمثل الأهداف الرئيسية لهذا المشروع في التحكم في الولوج إلى الموارد الحيوية لمركز بياناتهم وإمكانية التتبع الكاملة للمستخدمين ذوي الإمتيازات

Introduction générale

1. Contexte et problématique

Les entreprises peuvent être attaquées de multiples et différentes manières, imprédictibles parfois. Néanmoins, les attaques les plus préjudiciables ont un point en commun : celui d'exploiter des comptes ou identités à forts privilèges. Du fait de leur nature, ces comptes disposent d'autorisations (ou droits) leur permettant de modifier considérablement un système, une application ou une base de données. Les actions entreprises par le biais de ces comptes peuvent se révéler exceptionnellement destructrices.

Dans l'esprit de la plupart des gens, le terme « menaces internes » évoque un employé ou un administrateur IT mécontent qui cherche à se venger en causant des dommages ou en volant et en vendant des informations sensibles. Si ce risque peut devenir réalité, il n'est pas le seul. Des employés naïfs peuvent être le point d'entrée dans le réseau de personnes malveillantes et malignes venant de l'extérieur. Les ruses et techniques d'ingénierie sociale telles que l'hameçonnage (attaques ciblées) peuvent permettre à des personnes extérieures à l'entreprise d'obtenir des mots de passe et l'accès à des ressources internes normalement réservées à des collaborateurs de confiance.

2. Objectif

Pour véritablement réduire ses risques, l'entreprise doit aller au-delà du simple contrôle des accès à ses comptes à forts privilèges : elle peut notamment utiliser des contrôles d'accès très fins, afin d'être à même de contrôler ce qu'une personne qui est parvenue à se connecter à un compte peut faire. Elle peut également utiliser des contrôles d'identité afin d'implémenter des règles d'accès selon le « principe du moindre privilège » et de « séparation des fonctions ». Le suivi des actions réalisées sous un compte partagé et leur association à des utilisateurs spécifiques peut aussi contribuer à responsabiliser des utilisateurs habituellement anonymes. C'est dans cette optique que ce projet est inscrit.

Notre objectif consiste à concevoir et développer une application (solution) de traçabilité, d'audit et de contrôle des accès logique des administrateurs aux ressources critique, sans que les employer ne change leur méthode de travail quotidienne.

3. Organisation du mémoire

Ce document est organisé comme suit :

- Chapitre 1 : est un état de l'art des différents concepts relatif à la gestion des accès privilégié.

- Chapitre 2 : est dédié à l'analyse et la spécification des besoins, en détailleront aussi nos choix et aspect technique.

- Chapitre 3 : Ce chapitre décrit en détail la conception de notre solution.

- Chapitre 4 : Ce chapitre sera consacré à la réalisation de notre solution.

Nous terminerons ce document avec une conclusion générale et des perspectives.

Chapitre I :

Gestion des accès privilégiés

1- Introduction

Les comptes privilégiés, comme les comptes d'utilisateurs classiques, disposent d'un ensemble d'informations d'identification valide permettant d'accéder à un système particulier ou à un système sur un réseau donné. Plus généralement, un accès à privilèges, ou accès « root », permet de modifier les configurations d'un système, d'installer et désinstaller des programmes, de créer ou supprimer des comptes d'utilisateurs, ou encore d'accéder à des données sensibles.

Ces comptes sont conçus pour être utilisé par les administrateurs système pour gérer ou dépanner les systèmes réseau, exécuter des services ou autoriser des applications à communiquer les uns avec les autres. L'inconvénient est que ces mêmes informations d'identification, qui sont utilisées pour aider à garder le bon fonctionnement de l'entreprise, peut facilement être utilisé par des attaquants ou des initiés malveillants pour causer des dommages importants au réseau et à l'organisation.

En termes de sécurité, il n'est évidemment pas raisonnable d'accorder de tels droits de façon inconditionnelle. C'est la raison pour laquelle les accès à privilèges doivent être contrôlés et supervisés. Tout comme il doit être possible de révoquer ces droits à tout moment.

Dans ce chapitre on va commencer par des petites définitions sur les déférents concepts relatives à ce rapport, par la suite en abordera quelque étude sur les accès privilégiés, leur danger pour les organisations et on finira par une étude sur le marché de la gestion des accès privilégier et une conclusion.

2- Concepts et définitions

2.1- Identité

Élément ou ensemble d'éléments permettant d'identifier une personne ou une machine de façon univoque. Il peut s'agir d'un élément à connaître, par exemple un mot de passe ou un numéro d'identification (ID) personnel ; d'un élément à avoir, par exemple une carte d'identification, un jeton de sécurité ou un jeton logiciel ; d'une caractéristique de la personne, par exemple une empreinte digitale ou rétinienne ; ou d'une combinaison de ces différents éléments. [1]

2.2- Accès

Information correspondant aux droits accordés à une identité. Ces droits d'accès aux informations peuvent être affectés à des utilisateurs pour leur permettre de réaliser différents niveaux d'opérations, par exemple : la copie, le transfert, l'ajout, la modification, la suppression, la révision, l'approbation, la lecture seule et l'annulation. [1]

2.3- Contrôle d'accès

Le contrôle d'accès représente une composante essentielle de la gestion des accès. Il consiste à vérifier si un sujet (personne ou dispositif) qui demande l'accès à un objet (fichier, base de données ou dispositif) possède, à cet égard, les autorisations nécessaires. [1]

Le contrôle d'accès a pour objectifs :

- ✓ De gérer et contrôler les accès logiques aux ressources informationnelles par des personnes ou des dispositifs ;
- ✓ De détecter les accès non-autorisés;
- ✓ De préciser les règles à observer en matière d'identification, d'authentification et d'autorisation d'accès des personnes ou des dispositifs;
- ✓ D'assurer la disponibilité de l'information en réduisant :

- Les attaques de déni de service;
- Les destructions ou les effacements non-autorisés;
- La propagation d'un code malicieux entre systèmes informatiques;

✓ D'assurer l'intégrité de l'information en réduisant :

- Les abus d'utilisation ou de modification;
- Les altérations par des utilisateurs non-autorisés ;
- les erreurs d'utilisation ;

✓ D'assurer la confidentialité de l'information en réduisant :

- Les accès non autorisés;
- Les divulgations involontaires;
- Les diffusions non autorisées.
- D'assurer la traçabilité des accès et des tentatives d'accès.

2.4- Principe du privilège minimal

Le principe du privilège minimal exige que l'utilisateur ne dispose pas de plus de droits que nécessaire pour accomplir ses tâches. Cela implique que les autorisations accordées à un rôle constituent le strict minimum nécessaire à l'accomplissement des tâches associées à ce rôle. [1]

3- L'accès privilégié : ses avantages et ses risques

Quand il s'agit d'accéder et de manipuler des systèmes informatiques particulièrement précieux pour l'entreprise, les utilisateurs privilégiés tels que les administrateurs ont typiquement la plus large latitude opérationnelle qui soit. En général, les utilisateurs **l**es plus chevronnés au sein d'un département informatique sont responsables du déploiement et de la gestion des fonctionnalités dont dépend l'entreprise, allant des tâches quotidiennes essentielles aux fonctionnalités stratégiques qui permettent à l'entreprise de maintenir son avance sur sa

concurrence. Ils peuvent également avoir une responsabilité considérable dans leur secteur d'activités comme la gestion des applications commerciales.

Mais ce pouvoir comporte des risques. La complexité de l'informatique est telle, que même les modifications effectuées par les salariés les plus chevronnés peuvent avoir des impacts inattendus et graves sur la disponibilité, l'exécution et/ou l'intégrité des ressources. Les personnes malveillantes, à l'intérieur de l'entreprise et en dehors, peuvent profiter de l'accès au niveau administrateur pour causer des sérieux dégâts dans les affaires d'une société. Etant donné la sophistication et la discrétion de plus en plus évoluées des attaques d'aujourd'hui réalisées par le biais de malware et autres méthodes, il est commun pour des pirates d'obtenir et d'exploiter de tels privilèges en usurpant l'identité d'un collaborateur digne de confiance. [2]

4- Différents types de comptes privilégiés

Les comptes privilégiés existent sous plusieurs formes dans un environnement d'entreprise et généralement doublent ou triplent le nombre des employés en volume. Cependant, ils présentent des risques de sécurité importants s'ils ne sont pas protégés, gérés et surveillés.

Les types de comptes privilégiés généralement trouvés dans un environnement d'entreprise incluent :[3]

Administrateurs systèmes : Pour presque tous les périphériques d'un environnement informatique, il existe un compte privilégié partagé avec des privilèges élevés et un accès sans entrave à ses systèmes d'exploitation, réseaux, serveurs et bases de données.

Fournisseurs tiers : Un accès privilégié est accordé pour effectuer une fonction de travail permettant aux fournisseurs de travailler sous anonymat. Une fois à l'intérieur, les fournisseurs tiers ont un accès illimité pour élever leurs privilèges d'accès aux données sensibles de l'organisation.

Hyperviseur ou Gestionnaire de serveur cloud : Les processus métier, tels que les finances, les ressources humaines et les achats, évoluent vers des applications Cloud, Exposant les actifs de l'entreprise à un risque élevé du aux large accès accordé aux administrateurs de Cloud.

Administrateurs d'applications ou de bases de données : Les administrateurs d'applications et de bases de données disposent d'un large accès pour administrer les systèmes auxquels ils sont affectés. Cet accès leur permet également de se connecter à pratiquement toutes les autres bases de données ou applications qui se trouvent Dans l'entreprise.

Utilisateurs professionnels : Les cadres supérieurs et le personnel informatique ont souvent un accès privilégié aux applications professionnelles et données sensibles. Dans les mains d'une mauvaise personne, ces informations d'identification donnent accès aux données financières de l'entreprise, à la propriété intellectuelle, et d'autres données sensibles.

Applications : Les applications utilisent des comptes privilégiés pour communiquer avec d'autres applications, scripts, bases de données, services Web et plus. Ces comptes sont souvent négligés et posent un risque important, car leurs informations d'identification sont souvent codées en statiques. Un hacker peut utiliser ces points d'attaque pour augmenter l'accès privilégié dans toute l'organisation.

5- Danger de sécurité lié aux comptes privilégiés

Un niveau élevé de privilèges permet aux utilisateurs d'effectuer une grande variété d'actions malveillantes, de l'utilisation abusive des données à la compromission complète du système. Les utilisateurs peuvent utiliser leur accès administratif pour dérober des données client et des informations financières sensibles afin de les vendre ou même simplement les divulguer en

ligne. Les comptes privilégiés peuvent également être utilisés pour modifier ou supprimer des données sensibles, ouvrant ainsi des possibilités de fraude. Les utilisateurs technophiles peuvent utiliser de tels comptes pour installer des portes dérobées ou des exploits leur permettant un accès complet au système. Les employés mécontents peuvent même réduire l'ensemble du système en modifiant les paramètres critiques.

Cependant, ce qui rend dangereux les comptes privilégiés, ce n'est pas l'étendue de leur accès, mais plutôt la facilité avec laquelle ils peuvent effectuer des actions malveillantes et la difficulté de les détecter. Avec un accès légitime aux données sensibles et aux paramètres du système, les actions malveillantes des utilisateurs privilégiés sont souvent indissociables de leur activité quotidienne. Ces utilisateurs peuvent facilement couvrir leurs traces, et même s'ils sont pris, ils peuvent simplement prétendre qu'ils ont fait une erreur. Par conséquent, les actions malveillantes d'utilisateurs privilégiés peuvent passer inaperçues pendant très longtemps, ce qui ne servira qu'à augmenter les dommages et les coûts de remédiation quand ils seront finalement découverts.

Il est également intéressant de noter que les attaques malveillantes ne sont pas le seul danger en ce qui concerne les comptes privilégiés. Avec un niveau élevé de privilèges, les erreurs et les actions involontaires peuvent souvent être aussi coûteuses pour une entreprise qu'une attaque délibérée. Le simple fait d'envoyer par e-mail des données sensibles à la mauvaise personne peut entraîner des millions de dommages et frais de réparation.

Une autre grande préoccupation est la sécurité de ces informations d'identification. Si les auteurs parviennent à utiliser l'ingénierie sociale ou le piratage informatique pour obtenir un compte privilégié, ils auront accès à l'ensemble du système.

5.1- Source des menaces liées aux comptes à privilèges

Les menaces générées par les comptes à privilèges proviennent de trois sources de risques :

- **Menaces d'origine interne** : collaborateur malveillant, trop curieux.

- **Menaces d'origine externe** : pirate passionné, militant agissant de manière idéologique ou politique.

- **Menaces d'origine accidentelle** : erreur de configuration, de manipulation lors d'une mise à jour d'un système.

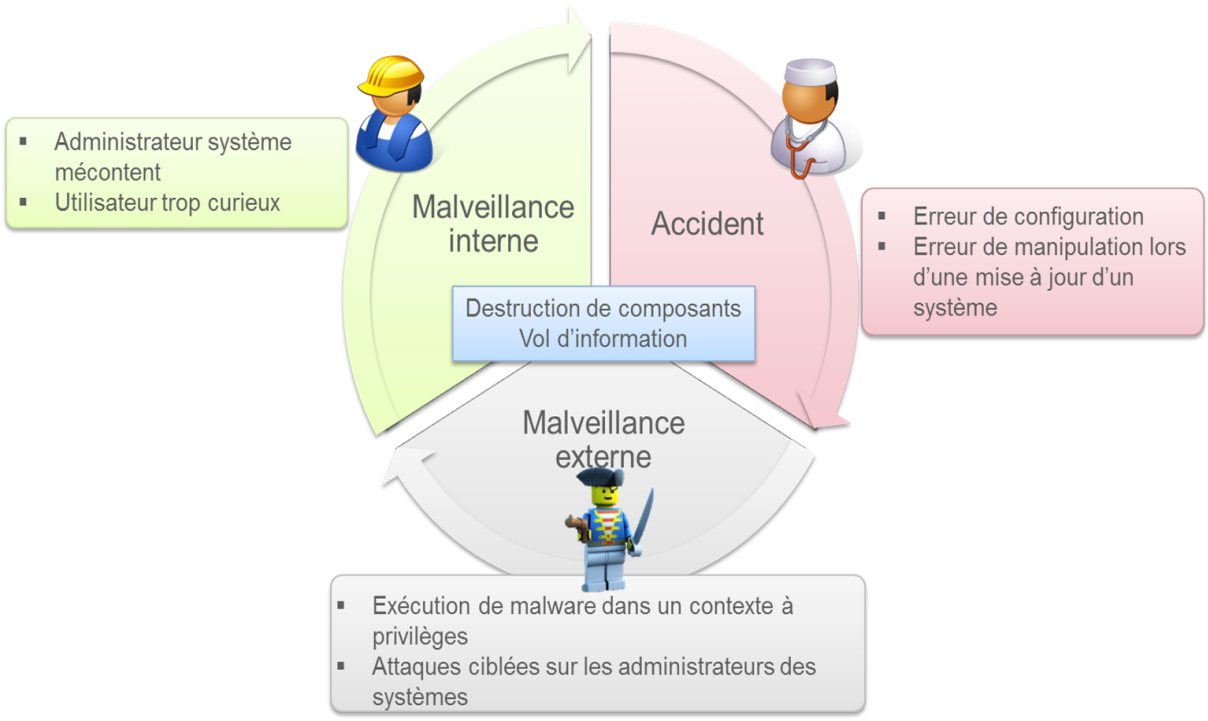


Figure 1 : Source des menaces liées aux comptes à privilèges [4].

5.2- Attaque sur les comptes privilégiés

Rappelons que les comptes privilégiés ne sont pas seulement ceux qui, disons, ont un accès administrateur à une base de données. Ils peuvent être un compte d'utilisateur normal avec des privilèges de niveau administrateur sur leur site local, poste de travail. Les attaquants utilisent tous les titres de compétences qu'ils peuvent obtenir en tant que des moyens potentiels pour réaliser un mouvement latéral. En supposant que l'attaquant a déjà quelques niveaux d'accès à un point de terminaison, il lui suffit de suivre un processus simple mais efficace: 1) Identifier et obtenir des informations d'identification avec un accès privilégié.

2) Accéder à un autre point de terminaison.

3) Répétez jusqu'à atteindre le système où se trouve l'ensemble de données souhaité.

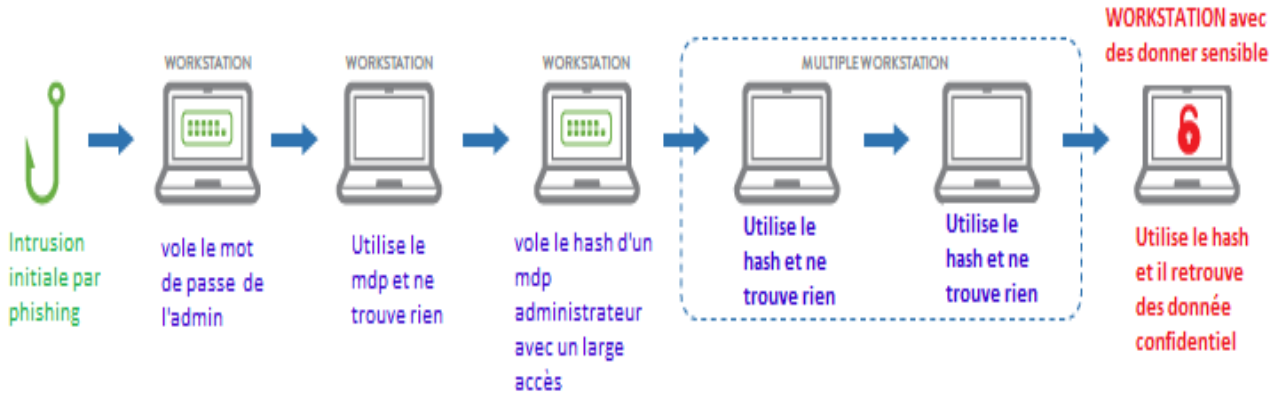


Figure 2: Exemple d'utilisation d'un compte privilégié

On peut penser à une attaque en trois couches - chacune représente un degré plus élevé de potentiel de menace pour une organisation:

Entrée : Le contrôle sur un point de terminaison est établi et utilisé comme point d'ancrage. Phishing, sites Web contenant des logiciels malveillants et exploitation de vulnérabilités connues sont les méthodes les plus courantes utilisées pour entrer.

Accès : Identifier et accéder aux informations d'identification qui ont des privilèges élevés via l'énumération des groupes, les tests des comptes locaux, et l'utilisation d'outils pour tirer les informations d'identification de la mémoire.

Activité : Mise en valeur des informations d'identification privilégiées trouvées, l'attaquant tente de se déplacer latéralement sur le réseau en accédant à des systèmes supplémentaires via des méthodes telles que RDP, WMI et PowerShell.

Rappelons que ces trois couches se produisent dans chaque attaque, ce qui rend le travail d'un IT un peu plus facile en identifiant comment mettre en place une défense correspondante pour chaque couche. Mais considérons également que les types spécifiques de logiciels malveillants utilisés et les actions entreprises peuvent varier et évoluer ce qui rend les menaces en constante évolution.

La réponse aux menaces potentielles d'une attaque externe doit exister sur les trois couches attaques, c'est-à-dire, avant qu'un attaquant ne gagne une sorte d'entrée dans l'organisation, et avant qu'ils puissent identifier les informations d'identification et essayer de les utiliser. Dans tous les cas. [5]

6- Modèle de gestion des identités et des accès

Le modèle de gestion des identités et des accès AAA est un cadre intégré dans le monde de la gestion des identités et des accès numériques pour gérer l'accès aux ressources et assurer la sécurité du système. AAA signifie Authentification, Autorisation et Traçabilité, que nous aborderons en détail ci-dessous. [6]

6.1- Authentification

L'authentification repose sur l'idée que chaque utilisateur aura une information unique qui le distingue des autres utilisateurs pour fournir une preuve d'identité lorsqu'ils s'identifient. Par exemple, vous entrez dans une zone surveillée et vous identifiez comme un employé ou un propriétaire de la zone surveillée. Ensuite, vous devez fournir une preuve pour authentifier la personne que vous prétendez être. Ce concept, associé au modèle de gestion des identités et des accès AAA, s'appliquera également aux périphériques IoT connectés.

Il existe principalement quatre types de méthodes d'authentification qui utilisent :

1. Les mots de passe statiques qui restent actifs jusqu'à ce qu'ils soient changés ou expirés,
2. Mot de passe à usage unique (OTP) comme les codes délivrés des textes SMS ou des jetons utilisés pour chaque session d'accès,
3. Certificat numérique,

4. Informations biométriques,

Les types d'authentification appartiennent à l'une des formes suivantes:

1. Quelque chose que vous connaissez comme un mot de passe;
2. Quelque chose que vous avez comme un porte-clés ou un téléphone portable; et
3. Quelque chose que vous êtes comme vos empreintes digitales, la voix, la géométrie de la main, etc. également appelé "authentification biométrique".

Lorsque nous combinons plusieurs de ces catégories, cela s'appelle l'authentification multi facteur (MFA), ce qui rend difficile l'authentification d'une autre personne. Par exemple, si un pirate vole le mot de passe d'un utilisateur, il doit aussi voler le téléphone portable pour accéder au code envoyé par le SMS ou posséder le porte-clés qui affiche le code qui se synchronise avec le code tournant dans le système en cours d'accès. L'utilisation de deux mots de passe n'est pas considérée comme 2FA car les deux mots de passe entrent dans la catégorie « quelque chose que vous connaissez ». C'est comme placer deux serrures sur une porte à la maison qui pourrait être ouverte avec la même clé.
La plupart des entreprises s'orientent vers l'authentification multi facteur (MFA) ou l'authentification à deux facteurs (2FA), qui s'appuie sur un mot de passe statique et OTP ou une question de défi pour renforcer la cyber sécurité.

6.2- Autorisation

L'autorisation est représentée par le second A du modèle de gestion des accès et des identités AAA qui consiste à accorder ou refuser à un utilisateur l'accès aux ressources système une fois que l'utilisateur a été authentifié par le nom d'utilisateur et le mot de passe. La quantité d'informations et la quantité de services auxquels l'utilisateur a accès dépendent du niveau d'autorisation de l'utilisateur.

Après que l'utilisateur s'identifie et soit authentifié pour prouver sa propriété de l'identité, il doit passer la règle d'autorisation pour accéder aux services, programmes et données du

système. L'autorisation détermine ce à quoi l'utilisateur peut accéder et à quoi il ne peut pas accéder.

Le principe du moindre privilège exige que les utilisateurs, les processus, les programmes et les périphériques ne puissent obtenir qu'un accès suffisant pour exécuter leurs fonctions requises, et rien de plus. Toute autorisation au-delà des fonctions normales du travail ouvre la porte à des violations accidentelles ou malveillantes des objectifs de sécurité; Confidentialité, intégrité et disponibilité. C'est l'une des principales raisons pour lesquelles les employés ne doivent pas avoir un accès administrateur ou racine aux dispositifs fournis par leur employeur, mais plutôt avoir un compte avec des privilèges limités en accord avec leurs exigences professionnelles. L'un des risques d'accorder aux employés l'accès administrateur aux dispositifs fournis par la société est que lorsque le dispositif est infecté par un virus, le logiciel malveillant fonctionnera avec les privilèges de l'utilisateur.

6.3- Traçabilité

Le troisième A du modèle de gestion des identités et des accès AAA fait référence à la Traçabilité qui consiste à suivre l'activité d'un utilisateur tout en accédant aux ressources du système, notamment le temps passé dans le réseau, les services consultés et le montant des données transférées pendant la session. Les données comptables sont utilisées pour l'analyse des tendances, la détection des tentatives de connexion infructueuses, la détection des violations de données, les enquêtes la planification de la capacité, la facturation, l'audit et la répartition des coûts.

Garder une trace des utilisateurs et de leurs activités sert à plusieurs fins. Par exemple, remonter à des événements menant à un incident de cyber sécurité peut s'avérer très utile pour une analyse criminalistique et une enquête.

En outre, surveiller les activités des employés qui pourraient être mécontents en raison d'événements de l'entreprise tels que les licenciements peuvent aider à détecter les tentatives de connexion échouées et à prédire quel type d'objectif malveillant ils pourraient avoir.

Pour être efficaces dans la comptabilité IAM, les comptes génériques et partagés doivent être évités afin que les actions de chaque individu puissent être prises en compte.

Pour détecter les fraudes et autres activités malveillantes, les entreprises peuvent envoyer des employés à des vacances obligatoires permettant au remplaçant de l'employé d'effectuer des vérifications et des soldes sur l'employé qui aurait caché ou dissimulé ses actions telles que des entrées de journal qui pourraient offrir à l'entreprise de nombreux indices sur les activités malveillantes de leurs employés.

7- Comparaison entre différentes solutions existantes

Un moyen infaillible de comprendre l'importance de sécuriser les comptes privilégiés est de commencer par des faits durs et froids. En évaluant les statistiques actuelles et celles projetées pour l'avenir, nous pouvons avoir une bonne idée de la nécessité d'une gestion de compte privilégiée et de l'orientation du marché.

Nous avons rassemblé un certain nombre de statistiques pour mener des recherches et des enquêtes qui démontrent à quel point la gestion des accès privilégiés peut avoir un impact sur la sécurité organisationnelle et comment le marché va changer et se développer dans les années à venir.

- **80%** Des failles de sécurité impliquent des informations d'identification privilégiées. [8]
- **82%** Des violations de données provoquées par des abus d'initiés ont pris plus d'une semaine à détecter. [9]
- **80%** Des professionnels de la sécurité informatique considèrent la sécurité de PAM comme une haute priorité [10]
- **66%** Des entreprises utilisent encore des méthodes manuelles pour gérer les comptes privilégiés. [10]
- **70%** Des organisations n'ont pas besoin d'approbation pour créer de nouveaux comptes privilégiés. [10]
- **50%** Des organisations n'auditent pas les comptes privilégiés. [10]

On va lister dans la section suivante de ce chapitre quelques fournisseurs de solution de gestion d'accès privilégiée (PAM) avec des profils individuels, des fonctionnalités clés et des références de capacité pour chacun.

7.1- BALABIT

La société de sécurité hongroise Balabit propose une suite de Solutions d'accès privilégié variable et dédiée Solutions de gestion, allant des solutions d'analyse de compte pour prévenir le vol d'identité Aux sessions privilégiées surveillées; La gestion de session privilégiée est capable de capturer Les frappes de l'utilisateur et les mouvements de la souris. Balabit utilise cette information pour nourrir son comportement moteur d'analyse, qui peut détecter le vol d'identité grâce à la biométrie comportementale. [11]

7.1.1- Principales caractéristiques

- **Analyse du comportement des utilisateurs en temps réel :** Intègre les données dérivées d'autres solutions et génère des profils de comportement qui sont continuellement utilisés pour identifier un comportement suspect.
- **Gestion des sessions privilégiées :** Contrôle l'accès privilégié aux systèmes informatiques distants, enregistre les activités dans les recherches, pistes de vérification de type vidéo, et empêche les actions malveillantes dans un dispositif déployable.
- **Intégration de solutions :** Balabit interagit avec les principales solutions de gestion de mots de passe pour fortifier les cyberdéfenses.
- **Visibilité profonde :** Peut surveiller des utilisateurs spécifiques accédant à l'infrastructure informatique et peut le faire en temps réel à partir de la date du journal.

7.1.2- Limites

Balabit est remarquable pour son moteur d'analyse du comportement de l'utilisateur, qui peut identifier l'activité du compte privilégié suspect. Cependant, le fournisseur manque de soutien pour la gestion des mots de passe d'application à application, ce qui limite sa viabilité pour les entreprises. Balabit est hautement considéré dans les secteurs financiers et publics; son intégration signifie qu'il est idéal pour les systèmes de sécurité hybrides pour les entreprises, mais les petites et moyennes entreprises ne peuvent se pas trouver, C'est le système de sécurité tout-en-un qu'ils devraient adopter.

7.2- CA Technologies

CA Technologies, dont le siège social est situé à New York, fournit des logiciels qui incluent non seulement la sécurité mais aussi le développement d'applications et la gestion de systèmes.

La société est devenue un acteur de Services PAM fin 2016 suite à l'acquisition de Xceedium et de leur solution XSuite PAM. CA Technologies fournit un accès contextuel / adaptatif à son produit Advanced Authentication, et offre CA API Management, un produit de gestion d'API à cycle de vie complet. CA Technologies dispose également d'une gouvernance et d'une administration de l'identité pour compléter ses outils PAM. [11]

7.2.1- Principales caractéristiques

- **Analyse des menaces :** CA Threat Analytics pour Privileged Access Manager permet aux entreprises d'évaluer continuellement les risques et détecter rapidement les activités malveillantes parmi ses utilisateurs privilégiés.
- **Accès à l'authentification unique (SSO) :** Active l'accès à connexion unique et l'identité fédérée pour les utilisateurs privilégiés, couvrant l'infrastructure d'entreprise hybride à travers le point de terminaison.
- **Option d'identité en tant que service (IDaaS) :** Permet l'adoption sécurisée du cloud, l'interface SSO et la gestion du cycle de vie de l'identité.

7.2.2-Limites

Les services PAM de CA Technologies sont encore relativement nouveaux sur le marché. Il faudra du temps pour développer des logiciels pour faire appel en dehors de leur base de clients existante. Leur solution est connue pour être complexe à gérer et difficile à déployer, mais s'adapte à la plupart des points de terminaison et s'intègre aux solutions IGA, SIEM et Security Analytics. Les petites et moyennes entreprises pourraient chercher une solution plus simple. Cependant, l'infrastructure mondiale d'empreinte et de support de CA Technologies le rend idéal pour les organisations multinationales à la recherche d'une solution évolutive pour les grands déploiements.

7.3- CyberArk

CyberArk, société de cybersécurité basée dans le Massachusetts, commande une part importante du Marché du PAM. Les solutions de sécurité de compte privilégiées de l'entreprise offrent une solution basée sur des règles qui sécurise, gère et enregistre les comptes et activités

privilégiés, et utilise l'analyse comportementale sur l'utilisation des comptes privilégiés pour détecter et signaler les anomalies. Les composants de PASS incluent un gestionnaire de clés SSH, Privileged Session Manager, Privileged Threat Analytics et Endpoint Privilege Manager. [11]

7.3.1- Principales caractéristiques

- **Gestionnaire de privilèges à la demande :** Élimine les privilèges root superflus et permet aux utilisateurs privilégiés d'exécuter des commandes administratives à partir de sessions natives.
- **Gestionnaire de session privilégié :** Isole, contrôle et surveille l'accès des utilisateurs privilégiés sur Unix, Linux, et les systèmes basés sur Windows, les bases de données et les machines virtuelles.
- **Analyse des menaces privilégiées :** Permet aux entreprises de détecter, d'alerter et de répondre aux attaques sur les comptes privilégiés en temps réel.

7.3.2- Limites

L'un des fournisseurs PAM les plus populaires sur le marché, CyberArk offre de puissantes capacités dans un ensemble intuitif. La prise en charge des plates-formes cloud est cependant limitée, de sorte que les leur solution avec CyberArk, mais il va séduire les grandes entreprises via sa réputation et son exhaustivité.

8- Conclusion

Les accès privilégiés représentent un grand danger pour les entreprises c'est pour cela qu'il ne faut pas laisser un tel accès sans contrôle, nous avons consacré ce chapitre a une étude sur ce type d'accès et son danger sur la sécurité d'une entreprise.

Dans le prochain chapitre on va introduire les différents concepts de notre solution.

Chapitre 2:

Analyse et spécification des besoins

1- Introduction

L'analyse et la spécification des besoins représentent la première phase du cycle de développement d'un logiciel. Nous commençons ce chapitre par la présentation de l'organisme d'accueil ou c'est dérouler notre stage de fin d'étude, par la suite nous allons aborder les différents besoins fonctionnels et non fonctionnel définit par l'organisme d'accueil, nous aborderont aussi les diffèrent aspect technique de notre projet.

2- Présentation de l'organisme d'accueille

2.1- Présentation du groupe SONELGAZ

SONELGAZ, acronyme de Société nationale de l'électricité et du gaz, est une compagnie chargée de la production, du transport et de la distribution de l'électricité et du gaz en Algérie.

Née en 1947 sous le nom 'Électricité et gaz d'Algérie (EGA)' et rebaptisée SONELGAZ en 1969, elle a depuis détenus le monopole du transport de l'électricité ainsi que la distribution et la vente de l'électricité et du gaz naturel dans notre pays.

Grace à sa ressource humaine formée et qualifiée, le groupe occupe une position privilégiée dans l'économie du pays en tant que responsable de l'approvisionnement de plus de six millions de ménages en électricité et de trois millions en gaz naturel, soit une couverture géographique de près de 99% en taux d'électrification et 52% pour la pénétration du gaz.

SONELGAZ vit depuis quelques années une phase particulièrement importante de son histoire. Désormais, la restructuration de SONELGAZ suite à la promulgation de la loi N°01.02 du 05 février 2002 s'est achevée avec la création de l'ensemble des filiales.

2.2- Missions du groupe SONELGAZ

SONELGAZ a pour mission principale la production, le transport et la distribution de l'électricité ainsi que le transport et la distribution du gaz par canalisation.

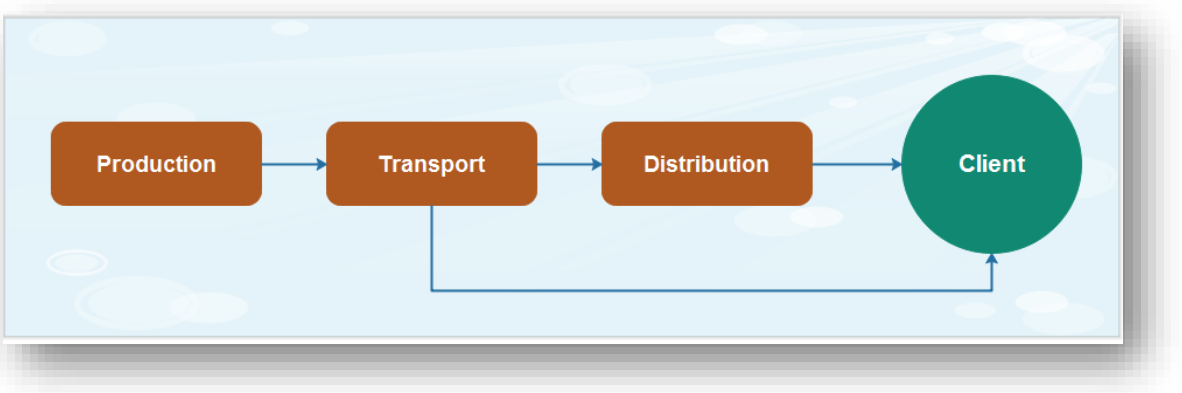


Figure 3 : *Missions du groupe SONELGAZ*

Selon le type d'énergie, le processus d'acheminement se définit comme suit :

a- *Pour l'électricité*

La production de l'électricité est un processus donnant lieu à l'énergie électrique. Cette dernière peut être produite à partir de différentes énergies sous différentes formes. La production se fait dans des centrales spécialisées.

Le transport permet d'acheminer l'électricité sur les grands axes du réseau électrique jusqu'au lieu de distribution ainsi que de contrôler l'équilibre global du système électrique.

La distribution consiste à distribuer jusqu'aux clients finaux l'électricité acheminée grâce aux grandes lignes du réseau de transport.

b- *Pour le gaz*

Le transport peut s'opérer soit par canalisation soit sous forme liquide dans des navires spécialisés. Le transport par canalisation reste la voie la plus privilégiée et consiste à acheminer ce dernier de la source de production ou d'importation via un réseau de canalisation jusqu'aux postes de transport. Pour la distribution du gaz, les clients ne sont pas directement raccordés aux réseaux de transport, les postes de transport se chargent de la distribution du gaz via d'autres réseaux.

2.3- Les sociétés en participation

SONELGAZ détient également des participations dans des sociétés différentes et ceci dans le cadre de promouvoir sa stratégie de diversification et d'entreprenariat.

Le but est de:

- Réaliser ses investissements grâce à l'apport de capitaux.
- Intégrer la technologie et le savoir-faire.
- Introduire l'expertise managériale dans les domaines de la gestion.

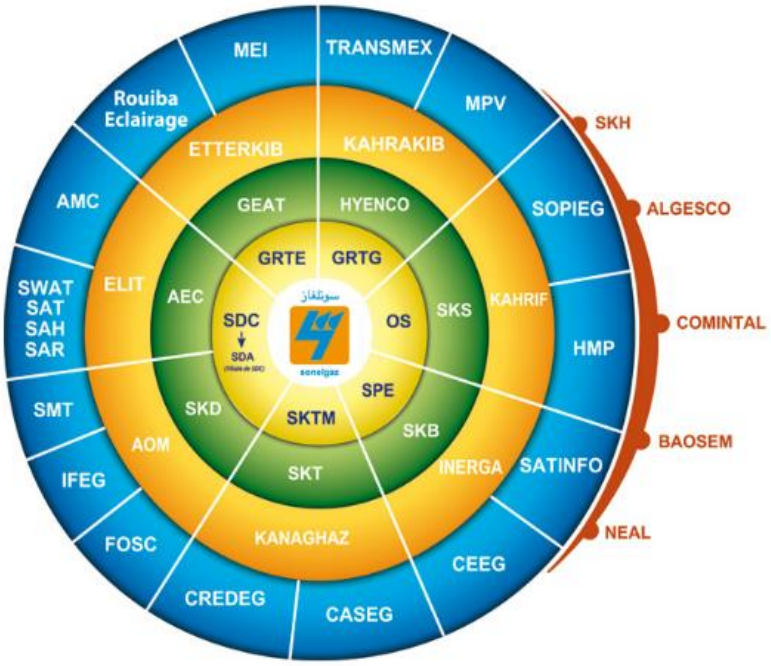


Figure 4 : Filiales du groupe SONELGAZ

2.4- Présentation de la société ELIT

Le 1er janvier 2009, l'activité liée au système d'information, qui était éparpillée dans différents départements auparavant au niveau de différentes directions tels que la direction des ressources Humaines et la direction de comptabilité, a été confiée à une nouvelle direction générale de SONELGAZ, dénommée DGSI Direction générale des systèmes d'information, filialisée ensuite en une société à part entière « EL Djazair Information Technology », par abréviation « ELIT Spa ».

2.5- Missions et attributions

La société EL Djazair Information Technology est chargée de définir et de mettre en œuvre la politique générale du groupe SONELGAZ concernant les systèmes d'information et les technologies de l'information et de la communication. Les missions assignées à ELIT se déclinent à deux niveaux, stratégiques et opérationnels. Pour le premier, ELIT contribue à la stratégie de groupe SONELGAZ par :

- L'élaboration de la politique des systèmes d'information et des technologies de l'information et de la communication du groupe SONELGAZ.
- La prise en charge des besoins des sociétés du groupe SONELGAZ en matière d'informatique et de télécommunication.

Quant au niveau opérationnel, ELIT s'emploie à :

- Élaborer et mettre en œuvre les systèmes d'informations destinées au pilotage et à la gestion des différentes activités des sociétés du groupe SONELGAZ.
- Mettre à la disposition des sociétés du groupe SONELGAZ, les moyens informatiques et de télécommunication (logiciels, matériel, infrastructure, etc.…) nécessaires pour assurer le niveau de service attendu.
- Assurer la maintenance et l'administration des systèmes d'information, des plateformes et des équipements mis à la disposition des utilisateurs.
- Assurer l'accès à l'information et aux applications et en garantir la sécurité, l'intégrité et la fiabilité.
- Mettre à la disposition des utilisateurs, l'expertise technique indispensable à la satisfaction de leurs besoins.
- Proposer à terme tous les services IT construits pour les sociétés du groupe aux clients externes.

2.6- Organisation d'ELIT

La macrostructure de la société ELIT est comme suit :

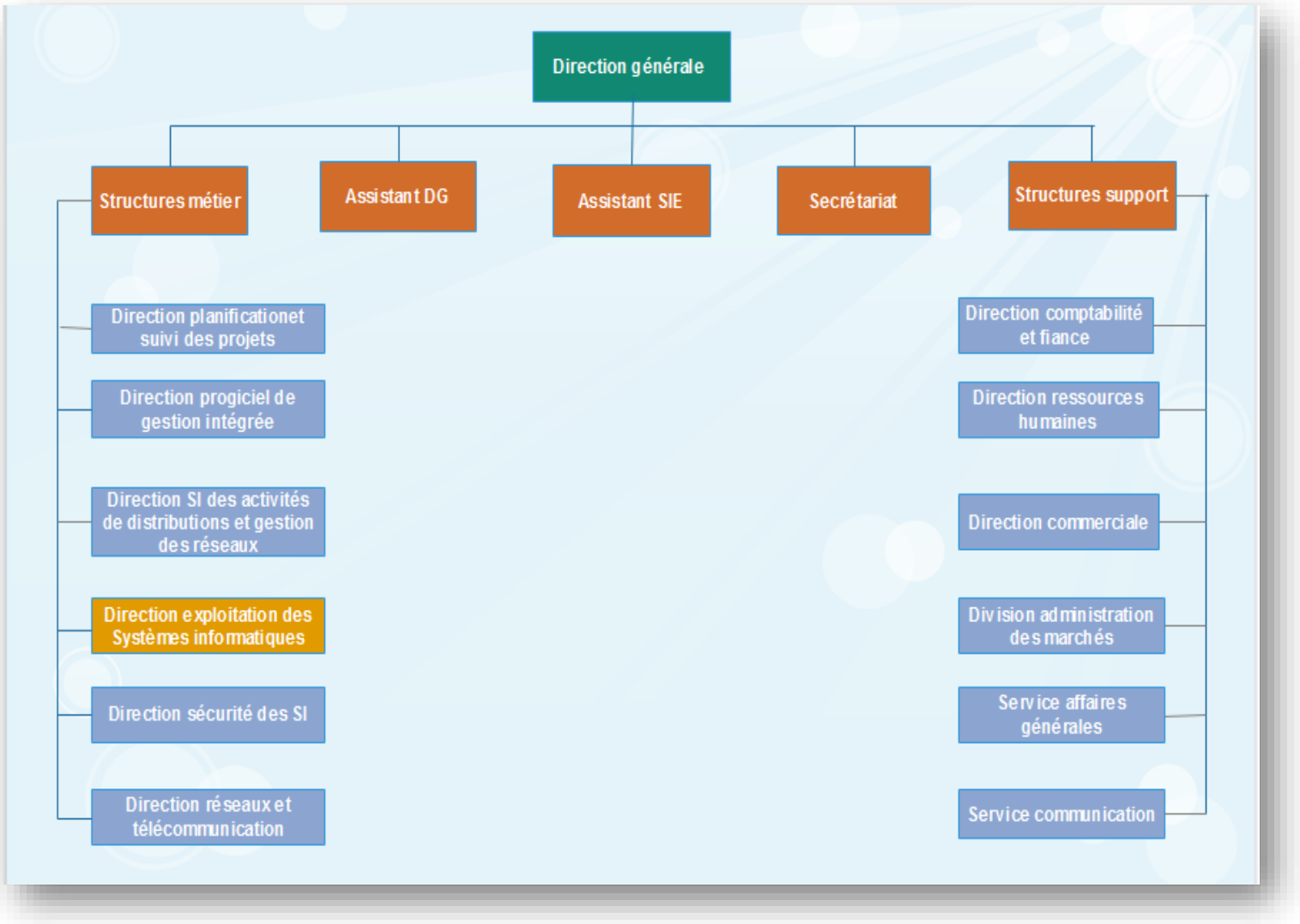


Figure 5 : *Structure organisationnelle d'ELIT.*

2.7- Structure d'accueil

Le stage de fin d'étude s'est déroulé au niveau du département rattaché à la direction de l'exploitation des systèmes d'information. Celle-ci est chargée de :

- L'exploitation et l'administration des systèmes, SGBD, applications et services composant le système d'information du groupe.
- La gestion des Datacenter qui sont des salles d'hébergement des équipements du Système d'Information du groupe.
- L'acquisition des équipements informatiques pour les entités du groupe.

Le support et l'assistance (via un Help Desk) des entités du groupe.

3- Analyse et spécification des besoins

3.1- Caractéristique de la solution

- ✓ La solution proposée doit pouvoir être déployée dans un environnement virtuel/physique.
- ✓ Le déploiement de la solution doit être sans agent (ni sur les ressources cibles, ni sur les postes clients).
- ✓ La solution proposée doit être administrée par une interface web.
- ✓ La solution doit supporter simultanément les protocoles :
    - Utilisateur vers la solution : http/https.
    - La solution vers les ressources cibles : SSH.

3.2- Besoins fonctionnels

3.2.1- Traçabilité

- ✓ Traçabilité totale de toutes les actions d'administration de la solution.
- ✓ Visualisation en temps réel du contenu des sessions actives.
- ✓ Visualisation en temps réel de l'historique des connexions et des authentifications.
- ✓ L'enregistrement des toutes les actions effectuées sur les ressources cibles doit être en format texte pour les accès en ligne de commande (SSH).
- ✓ Recensement des connexions (qui s'est connecté ?, a quelle ressource ?, combien de temps ? et comment ?.
- ✓ Recherche par mots clé sur les enregistrements.

3.2.2- Authentification et contrôle d'accès

- ✓ Support de l'accès unique des utilisateurs aux différentes ressources cibles (SSO, pour Single Sing On)

- ✓ La synchronisation périodique avec active Directory.
- ✓ Conformité aux exigences d'une politique des mots de passe (générer un mot de passe complexe).
- ✓ Déconnexion en temps réel des utilisateurs lors d'une manipulation non autorisée.
- ✓ Les sessions inactives doivent être verrouillées automatiquement au bout d'une valeur paramétrable.
- ✓ Connexion simultanée d'un utilisateur a plusieurs sessions.

3.3- Besoins non fonctionnels

Les besoins non fonctionnels concernent les contraintes à prendre en considération pour mettre en place une solution adéquate aux attentes des concepteurs des architectures dynamiques.

Notre application doit nécessairement assurer ces besoins :

- ✓ **L'extensibilité**

Dans le cadre de ce travail, l'application devra être extensible, c'est-à dire qu'il pourra y avoir une possibilité d'ajouter ou de modifier de nouvelles fonctionnalités.

- ✓ **La sécurité**

L'application doit être hautement sécurisée, les informations ne doivent, pas être accessibles à tout le monde.

- ✓ **La performance**

L'application doit être performante c'est-à-dire que le système doit réagir dans un délai précis, quel que soit l'action d'utilisateur.

4- Solutions pour tracer et contrôler l'accès aux systèmes d'informations

4.1- Le socle central d'accès

Le socle central d'accès constitue l'élément central du SI par lequel circulent les flux en provenance des utilisateurs (interne, externe, administrateur) et en direction des environnements de production, une sorte de relais entre l'utilisateur/administrateur et les données de l'entreprise.

Il devient ainsi très important de faire le choix d'un mécanisme d'accès à ce socle central, élément stratégique et sensible du système d'information. Ce mécanisme d'accès permettra de contrôler l'accès au socle pour administrer les serveurs de production, les équipements réseaux et les flux, ce qui ne va pas sans impacts sur l'architecture du système d'information. La solution choisie doit donc prendre en compte l'environnement technique, les habitudes des administrateurs et des logiciels historiquement utilisés. [4]

4.2- Le mécanisme de contrôle d'accès distribué

Une alternative au système de gestion d'accès centralisé consiste à disposer d'identités réparties sur de nombreux systèmes différents. Il s'agit de l'arrangement par défaut pour de nombreuses organisations qui ajoutent de nouvelles applications à leur organisation et utilisent simplement les contrôles d'accès et de gestion des utilisateurs par défaut ou intégrés. Cela se traduit généralement par le fait que les employés doivent jongler avec plusieurs noms d'utilisateur et mots de passe, qui auront souvent des exigences de complexité de mot de passe différentes , avec des exigences de fréquence de mise à jour différentes et des processus de réinitialisation différents pour chaque système. Et ce ne sont là que quelques-uns des défis que pose un système distribué aux utilisateurs.

4.3- Comparaison entre le mécanisme de contrôle d'accès centralisé et distribué

Une gestion centralisée des accès est généralement plus sécurisée car elle permet une gestion unifiée des identités et des profils, unifie et simplifie les systèmes de sécurité d'une entreprise, facilitant ainsi la gestion et la maintenance des contrôles d'accès dans l'entreprise. Grâce à un système d'authentification centralisé, les utilisateurs peuvent accéder à tous leurs programmes de travail et à leurs ressources via un ensemble unique d'identifiants de connexion. Cependant, la gestion centralisée des accès signifie également un point de défaillance unique. Un pirate informatique doit uniquement violer un jeu de références pour accéder à tout ce à quoi l'utilisateur piraté peut accéder.

Les administrateurs sont confrontés à toute une série de défis lorsqu'ils traitent des systèmes de gestion des accès distribués. Ils doivent gérer les utilisateurs pour chaque système individuel. Ils doivent apprendre l'étendu des autorisations pour chaque ressource et pour chaque utilisateur. Lorsqu'un employé quitte l'entreprise ou déménage vers un nouveau poste avec différents besoins d'accès aux données, il doit désactiver ou mettre à jour les profils individuels de l'utilisateur sur tous les différents systèmes.

La seule chose que l'on puisse dire en faveur d'un système distribué est que les données sont réduites au silence, ce qui signifie que si le mot de passe d'un utilisateur est volé sur un système, le voleur ne pourra pas nécessairement accéder aux autres systèmes. D'autre part, de nombreux utilisateurs réutilisent les mots de passe sur leurs comptes. Ce n'est pas une pratique sûre par tous les moyens, mais c'est malheureusement très courant.

La plupart des utilisateurs avancés en informatique utilisent leur poste personnel pour se connecter vers des serveurs de travail distants qui sont dans de nombreux cas extérieurs à leur réseau local.

Le protocole standard de connexion dans ce cas est le SSH pour Secured SHell (terminal sécurisé).

Utiliser ce type de connexion peut être relativement fréquent lors d'une journée de travail classique derrière un ordinateur, la copie et/ou la récupération de données, configuration, administration sur une machine extérieure au réseau local auquel appartient le poste de travail devient alors quelque chose de routinier.

L'évolution des conditions de sécurité est telle que les connexions entre les ressources d'un réseau local et des machines situées en dehors de ce réseau (sur le web) sont de plus en plus souvent centralisées et filtrées par une machine appelée ' Server proxy'.

5- Serveur Proxy

Un serveur proxy, également appelé "proxy" ou "passerelle au niveau de l'application", est un ordinateur qui fait office de passerelle entre un réseau local (par exemple, tous les ordinateurs d'une entreprise ou d'un bâtiment) et un serveur à plus grande échelle (réseau tel qu'internet), Les serveurs proxy fournissent des performances et une sécurité accrue. Dans certains cas, ils surveillent l'utilisation des ressources externes par les employés.

Un serveur proxy fonctionne en interceptant les connexions entre l'expéditeur et le destinataire. Toutes les données entrantes entrent par un port et sont transmises au reste du réseau via un autre port. En bloquant l'accès direct entre deux réseaux, les serveurs proxy font qu'il est beaucoup plus difficile pour les pirates d'obtenir des adresses internes et les détails d'un réseau privé. [12]

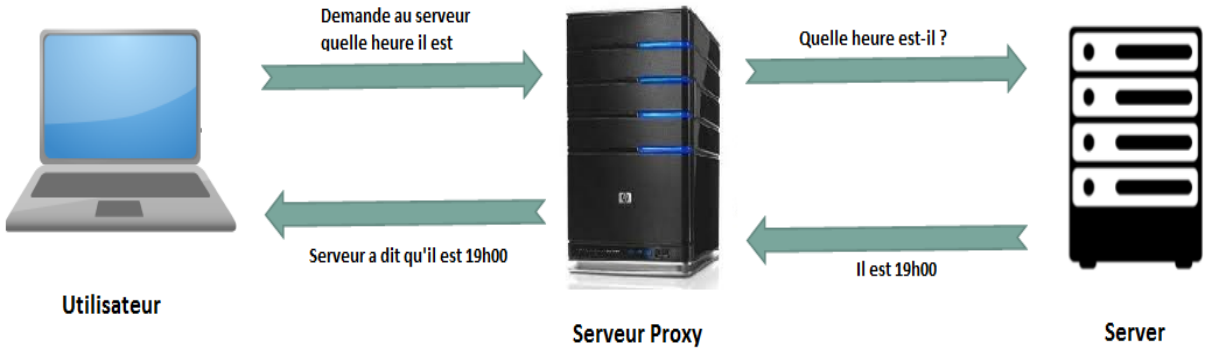


Figure 6 : *Principe d'un Serveur Proxy.*

6- Le Protocol SSH

SSH, ou Shell sécurisé, est un protocole sécurisé et le moyen le plus courant d'administrer en toute sécurité des serveurs distants. En utilisant un certain nombre de technologies de cryptage, SSH fournit un mécanisme pour établir une connexion cryptographiquement sécurisé entre deux parties, en authentifiant chaque côté à l'autre, et en transmettant des commandes et des sorties dans les deux sens.[13]

6.1- Utilisation de SSH

L'accès distant à un serveur de manière sécurisée est la fonction principale du protocole SSH, mais il est également intéressant de voir qu'il présente d'autres fonctionnalités qui sont aujourd'hui très utilisées. [13]

- **Transfert de fichier sécurisé :**

SSH permet également le transfert de fichier entre des machines de manière sécurisée, le protocole FTP permettant le transfert de fichier entre deux machines, n'est pas sécurisé. Il laisse en effet passer les informations de connexion, mais également les fichiers transférés, en clair sur le réseau. On est alors capable de récupérer, en plus des identifiants, le contenu des fichiers. Le protocole SSH permet de sécuriser les transferts de fichier, notamment via la commande *SCP*, le *SFTP* ou encore le *SSHFS* :

- **SCP** : Secure Copy
- **SFTP** : SSH File Transfert Protocol
- **SSHFS** : SSH File System

Une autre utilisation qui peut être faite du protocole SSH est le X Forwarding. Sous Linux, "X" est souvent employé pour parler du mode graphique ou GUI. Le protocole SSH permet en effet d'effectuer un transfert graphique du serveur vers le client. Autrement dit, on pourra lancer une application graphique sur le serveur, par exemple une visionneuse d'image, et la fenêtre et son contenu apparaîtra sur le poste du client, le tout étant transféré via SSH entre le serveur et le client.

- **Tunneling et encapsulation de protocole**

Le protocole SSH peut permettre l'encapsulation de n'importe quel protocole. Ainsi, un protocole non chiffré comme l'HTTP peut être encapsulé dans un le protocole SSH pour passer un pare-feu ou un proxy par exemple. Il sera ensuite désencapsuler à la destination On peut également entendre la description de "*Proxy SSH*" lorsque l'on parle de ce procédé de *tunneling SSH*.

Le fait que SSH dispose de plusieurs fonctionnalités lui permet d'être un outil très utile et très efficace lorsque l'on sait le maîtriser correctement. Il permet de se passer d'outils et de protocoles moins fiables et moins sécurisés tel que Telnet ou FTP.

6.2- Chiffrement utilisé dans le protocole SSH

Afin de sécuriser la transmission d'informations, SSH utilise un certain nombre de différents types de techniques de manipulation de données à différents moments de la transaction. Ceux-ci comprennent des formes de cryptage symétrique, de cryptage asymétrique et de hachage. [12]

6.2.1- Chiffrement symétrique

Le chiffrement symétrique est un type de chiffrement où une clé peut être utilisée pour crypter des messages à la partie adverse, et également pour déchiffrer les messages reçus de l'autre participant. Cela signifie que toute personne détenant la clé peut chiffrer et déchiffrer des messages à toute autre personne détenant la clé.

Ce type de schéma de cryptage est souvent appelé cryptage "secret partagé" ou cryptage "clé secrète". Il n'y a généralement qu'une seule clé qui est utilisée pour toutes les opérations, ou une paire de clés où la relation est facile à découvrir et il est trivial de dériver la clé opposée.

SSH utilise des clés symétriques pour chiffrer la totalité de la connexion. Contrairement à ce que certains utilisateurs supposent, les paires de clés asymétriques publiques / privées qui peuvent être créées ne sont utilisées que pour l'authentification, et non pour le cryptage de la connexion.

Le client et le serveur contribuent tous deux à l'établissement de cette clé, et le secret qui en résulte n'est jamais connu des parties extérieures. La clé secrète est créée à l'aide d'un processus connu sous le nom d'algorithme d'échange de clés. Cet échange a pour résultat que le serveur et le client arrivent tous les deux à la même clé indépendamment en partageant certaines données publiques et en les manipulant avec certaines données secrètes.

La clé de chiffrement symétrique créée par cette procédure est basée sur une session et constitue le chiffrement réel des données envoyées entre le serveur et le client. Une fois ceci établi, le reste des données doit être chiffré avec ce secret partagé. Ceci est fait avant d'authentifier un client.

SSH peut être configuré pour utiliser différents systèmes de chiffrement symétriques, notamment AES, Blowfish, 3DES, CAST128 et Arcfour. Le serveur et le client peuvent tous deux décider d'une liste de leurs chiffrements pris en charge, classés par préférence. La première option de la liste du client disponible sur le serveur est utilisée comme algorithme de chiffrement dans les deux directions. [13]

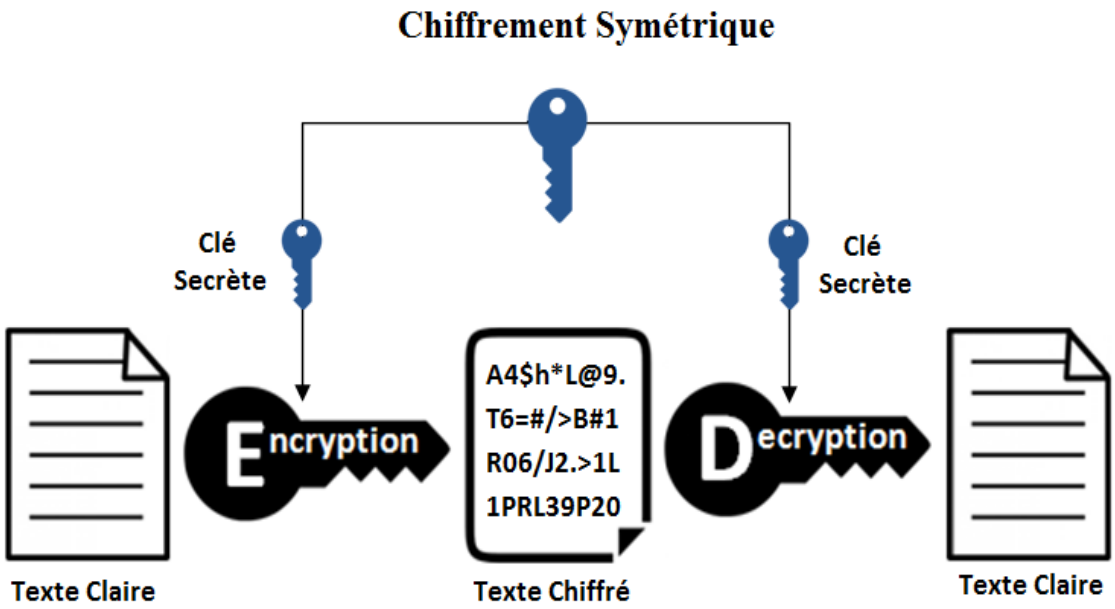


Figure 7 : Chiffrement symétrique.[25]

6.2.2- Chiffrement Asymétrique

Le chiffrement asymétrique est différent du chiffrement symétrique dans le sens ou pour envoyer des données dans une seule direction, deux clés associées sont nécessaires. L'une de ces clés est appelée clé privée, tandis que l'autre est appelée clé publique.

La clé publique peut être librement partagée avec n'importe quelle partie. Mais la clé privée ne peut pas être dérivée de la clé publique. La relation mathématique entre la clé publique et la clé privée permet à la clé publique de chiffrer les messages qui ne peuvent être décryptés que par la clé privée. C'est une capacité unidirectionnelle, ce qui signifie que la clé publique n'a pas la capacité de déchiffrer les messages qu'elle écrit, ni qu'elle peut déchiffrer tout ce que la clé privée peut lui envoyer.

La clé privée doit être gardée entièrement secrète et ne doit jamais être partagée avec une autre partie. Ceci est une exigence clé pour que le paradigme de clé publique fonctionne. La clé privée est la seule composante capable de déchiffrer les messages cryptés à l'aide de la clé publique associée.

SSH utilise le cryptage asymétrique dans quelques endroits différents. Pendant le processus d'échange de clés initial utilisé pour configurer le cryptage symétrique (utilisé pour crypter la session), un cryptage asymétrique est utilisé. A ce stade, les deux parties produisent des paires de clés temporaires et échangent la clé publique afin de produire le secret partagé qui sera utilisé pour le cryptage symétrique.

L'utilisation la plus explicite du cryptage asymétrique avec SSH provient de l'authentification par clé SSH. Les paires de clés SSH peuvent être utilisées pour authentifier un client auprès d'un serveur. Le client crée une paire de clés et télécharge ensuite la clé publique sur un serveur distant auquel il souhaite accéder. Ceci est placé dans un fichier appelé authorized_keys dans le répertoire (~ / .ssh) dans le répertoire personnel du compte utilisateur sur le serveur distant.

Une fois le chiffrement symétrique établi pour sécuriser les communications entre le serveur et le client, le client doit s'authentifier pour pouvoir accéder. Le serveur peut utiliser la clé publique dans ce fichier pour crypter un message de challenge au client. Si le client peut prouver

qu'il était capable de déchiffrer ce message, il a démontré qu'il possède la clé privée associée. Le serveur peut ensuite configurer l'environnement pour le client. [13]

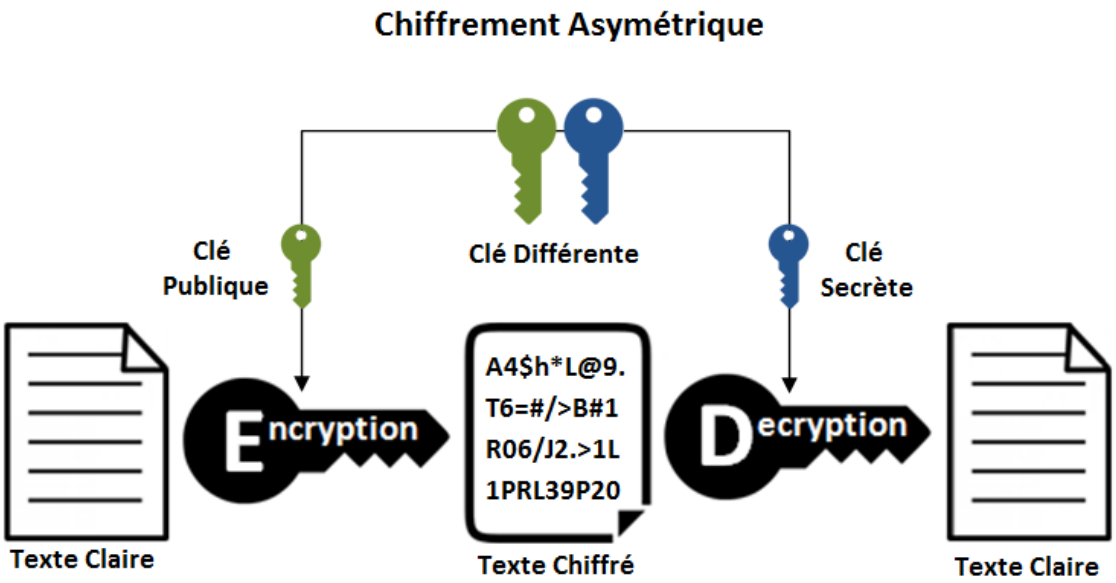


Figure 8 : Chiffrement Asymétrique.[25]

6.2.3- Hachage

Une autre forme de manipulation de données dont SSH profite est le hachage cryptographique. Les fonctions de hachage cryptographiques sont des méthodes de création d'une "signature" succincte ou d'un résumé d'un ensemble d'informations. Leurs attributs distinctifs principaux sont qu'ils ne sont jamais destinés à être inversés, ils sont pratiquement impossibles à influencer de façon prévisible, et ils sont pratiquement uniques.

Utiliser la même fonction de hachage et le même message devrait produire le même hachage; modifier toute partie des données devrait produire un hachage entièrement différent. Un utilisateur ne devrait pas être capable de produire le message original à partir d'un hachage donné, mais il devrait être capable de dire si un message donné a produit un hachage donné. Compte tenu de ces propriétés, les hachages sont principalement utilisés à des fins d'intégrité des données et pour vérifier l'authenticité de la communication. L'utilisation principale dans SSH

est avec HMAC, ou codes d'authentification de message basé sur le hachage. Ils sont utilisés pour s'assurer que le texte du message reçu est intact et non modifié.

Dans le cadre de la négociation de chiffrement symétrique décrite ci-dessus, un algorithme de code d'authentification de message (MAC) est sélectionné. L'algorithme est choisi en travaillant à travers la liste des choix MAC acceptables du client. Le premier de cette liste pris en charge par le serveur sera utilisé.

Chaque message envoyé après le cryptage doit contenir un MAC afin que l'autre partie puisse vérifier l'intégrité du paquet. Le MAC est calculé à partir du secret partagé symétrique, du numéro de séquence de paquet du message et du contenu réel du message.

Le MAC lui-même est envoyé en dehors de la zone chiffrée symétriquement en tant que partie finale du paquet. Les chercheurs recommandent généralement cette méthode de cryptage des données d'abord, puis de calculer le MAC. [13]

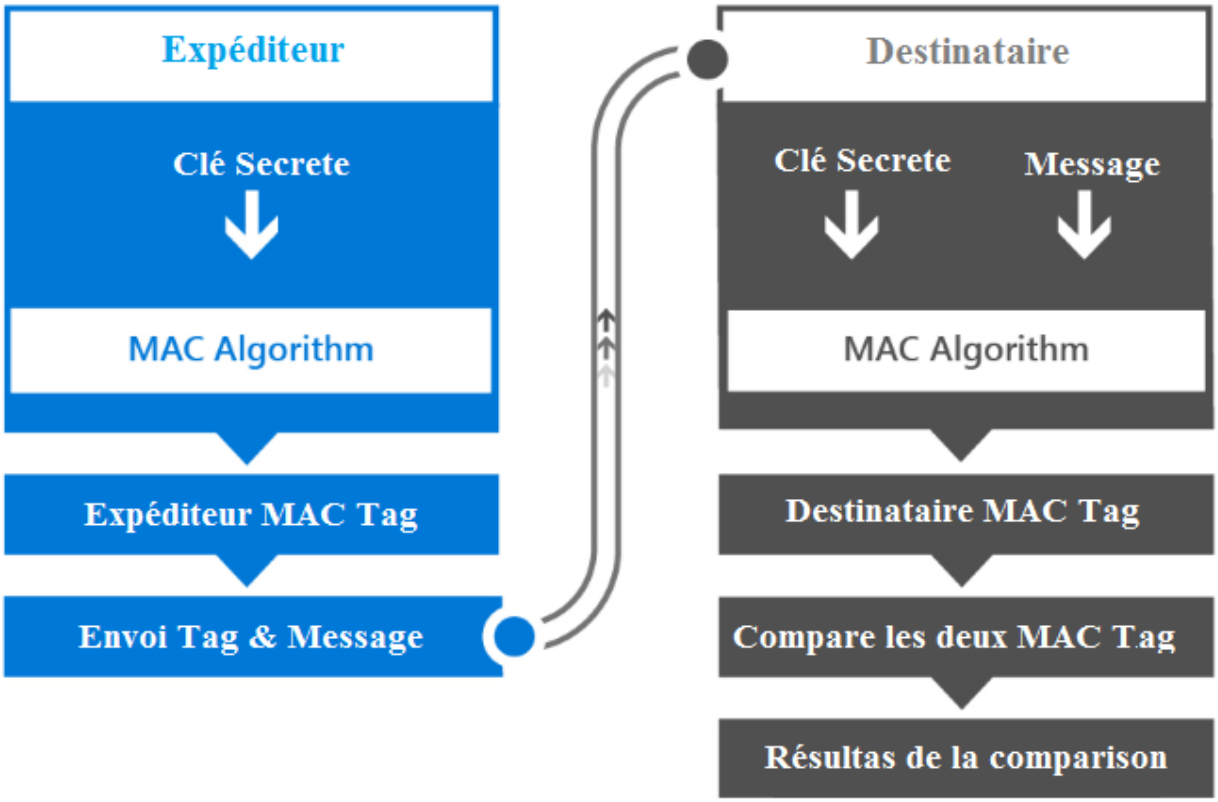


Figure 9 : *Algorithme de hachage MAC.*

6.2.4- Négociation du Cryptage de la session

Lorsqu'une connexion TCP est établie par un client, le serveur répond avec les versions de protocole qu'il prend en charge. Si le client peut correspondre à l'une des versions de protocole acceptables, la connexion continue. Le serveur fournit également sa clé d'hôte publique, que le client peut utiliser pour vérifier s'il s'agit de l'hôte prévu.

À ce stade, les deux parties négocient une clé de session en utilisant une version de quelque chose appelé l'algorithme Diffie-Hellman. Cet algorithme (et ses variantes) permet à chaque partie de combiner ses propres données privées avec des données publiques de l'autre système pour arriver à une clé de session secrète identique.

La clé de session sera utilisée pour chiffrer toute la session. Les paires de clés publiques et privées utilisées pour cette partie de la procédure sont complètement distinctes des clés SSH utilisées pour authentifier un client auprès du serveur.

La base de la procédure Diffie-Hellman classique est:

1- Les deux parties sont d'accord sur un grand nombre premier, qui servira de valeur de départ.
2- Les deux parties sont d'accord sur un générateur de cryptage (typiquement AES), qui sera utilisé pour manipuler les valeurs d'une manière prédéfinie.
3- Indépendamment, chaque partie arrive avec un autre nombre premier qui est gardé secret de l'autre partie. Ce numéro est utilisé comme clé privée pour cette interaction (différente de la clé privée SSH utilisée pour l'authentification).
4- La clé privée générée, le générateur de chiffrement et le nombre premier partagé sont utilisés pour générer une clé publique dérivée de la clé privée, mais qui peut être partagée avec l'autre partie.
5- Les deux participants échangent ensuite leurs clés publiques générées.
6- L'entité réceptrice utilise sa propre clé privée, la clé publique de l'autre partie et le nombre premier partagé d'origine pour calculer une clé secrète partagée. Bien que cela soit calculé indépendamment par chaque partie, en utilisant des clés privées et publiques opposées, il en résultera la même clé secrète partagée.

7- Le secret partagé est ensuite utilisé pour chiffrer toutes les communications qui suivent.

Le chiffrement secret partagé utilisé pour le reste de la connexion est appelé protocole de paquet binaire. Le processus ci-dessus permet à chaque partie de participer également à la génération du secret partagé, ce qui ne permet pas à une extrémité de contrôler le secret. Il accomplit également la tâche de générer un secret partagé identique sans jamais avoir à envoyer cette information sur des canaux non sécurisés. Le secret généré est une clé symétrique, ce qui signifie que la même clé utilisée pour chiffrer un message peut être utilisée pour le déchiffrer de l'autre côté. Le but de ceci est d'envelopper toute autre communication dans un tunnel crypté qui ne peut pas être déchiffré par des étrangers. Une fois le chiffrement de session établi, l'étape d'authentification de l'utilisateur commence. [13]

7- Active Directory

Active Directory est un annuaire LDAP pour les systèmes d'exploitation Windows, créé par Microsoft. Cet annuaire contient différents objets, de différents types (utilisateurs, ordinateurs, etc.), l'objectif étant de centraliser deux fonctionnalités essentielles : l'**identification** et l'**authentification** au sein d'un système d'information.

Depuis Windows Server 2000, le service d'annuaire Active Directory ne cesse d'évoluer et de prendre de l'importance au sein des organisations dans lesquelles il est mis en place. De ce fait, il est notamment utilisé pour le déploiement de stratégie de groupe, la distribution des logiciels ou encore l'installation des mises à jour Windows. [14]

7.1- Les intérêts d'un annuaire

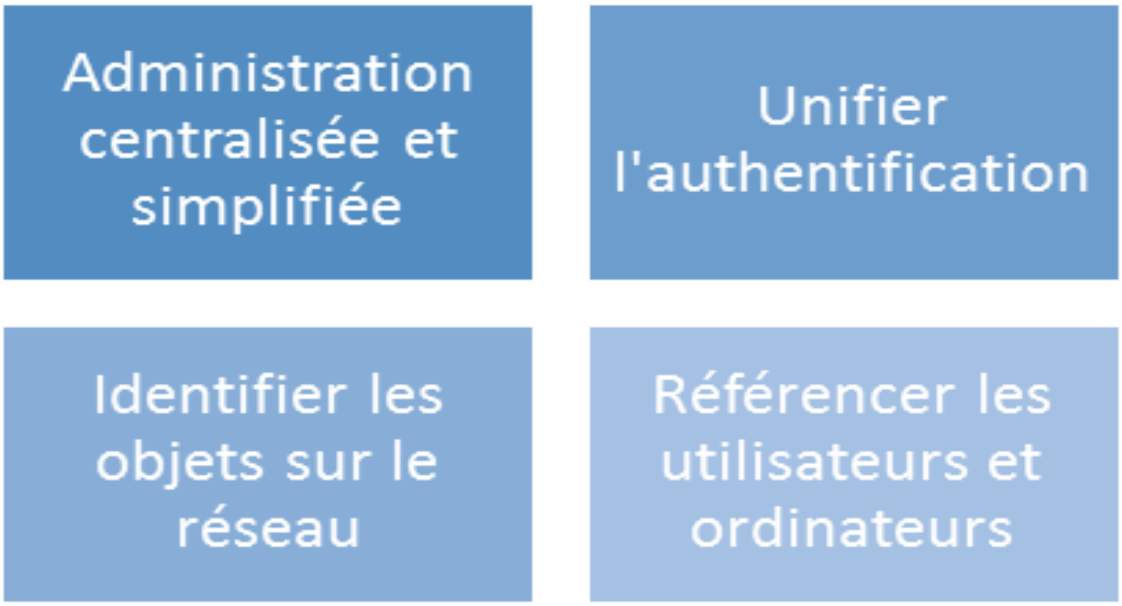


Figure 10 : *Les intérêts d'un annuaire.*

- **Administration centralisée et simplifiée** : la gestion des objets, notamment des comptes utilisateurs et ordinateurs est simplifiée, car tout est centralisé dans l'annuaire Active Directory. De plus, on peut s'appuyer sur cet annuaire pour de nombreuses tâches annexes comme le déploiement de stratégies de groupe sur ces objets.
- **Unifier l'authentification** : un utilisateur authentifié sur une machine, elle-même authentifiée, pourra accéder aux ressources stockées sur d'autres serveurs ou ordinateurs enregistrés dans l'annuaire (à condition d'avoir les autorisations nécessaires). Ainsi, une authentification permettra d'accéder à tout un système d'information par la suite, surtout que de nombreuses applications sont capables de s'appuyer sur l'Active Directory pour l'authentification. Un seul compte peut permettre un accès à tout le système d'information, ce qui est fortement intéressant pour les collaborateurs.
- **Identifier les objets sur le réseau** : chaque objet enregistré dans l'annuaire est unique, ce qui permet d'identifier facilement un objet sur le réseau et de le retrouver ensuite dans l'annuaire.

- **Référencer les utilisateurs et les ordinateurs** : l'annuaire s'apparente à une énorme base de données qui référence les utilisateurs, les groupes et les ordinateurs d'une entreprise. On s'appuie sur cette base de données pour réaliser de nombreuses opérations : authentification, identification, stratégie de groupe, déploiement de logiciels, etc. [14]

8- Conclusion

Dans ce chapitre nous avons abordé la partie présentation générale de l'entreprise ensuite nous avons énuméré les diffèrent besoin fonctionnel et non fonctionnel que notre system doit répondre. En plus nous avons présenté les diffèrent aspect technique de notre projet, Ce chapitre a été crucial pour la compréhension des fonctionnalités de notre system.

Le chapitre suivant sera consacré à la conception de notre solution.

Chapitre 3 : Conception

1- Introduction

La démarche de conception est une étape fondamentale dans le processus de développement puisqu'elle fait correspondre la vision applicative (le modèle d'analyse) à la vision technique (l'environnement de développement et d'exécution).

Ce chapitre vise à illustrer la phase de conception et les modèles UML associés. Nous commençons par un schéma global de notre solution, puis établir les diagrammes de cas d'utilisation et les diagrammes de séquences associé, ensuite nous élaborons le diagramme de classe, suivi du passage de ce dernier au Schéma relationnelle de la base de données.

2- Présentation de la solution

La figure suivante représente l'architecture globale de notre solution proposée.

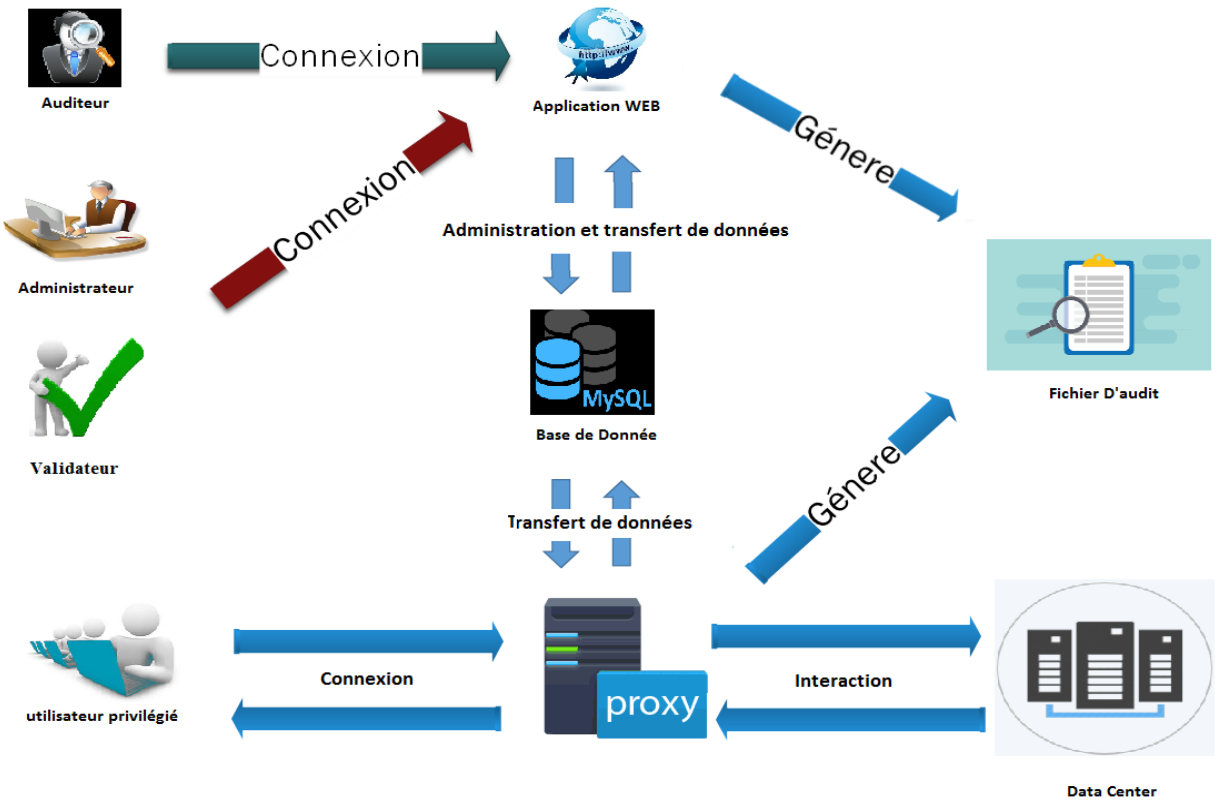


Figure 11 : Architecture globale du système.

Comme montré sur le schéma ci-dessus, on a choisi d'utiliser un serveur proxy comme notre mécanisme d'accès centralisé pour différentes raisons :

- Simplicité et la facilité d'accès au ressource cible.
- Serveur Proxy accélère les données de navigation et d'accès en raison de son système de cache.
- Permettre un contrôle total sur le réseau et les protocoles utiliser.
- Permettre une analyse complète sur le trafic ce que nous aide pour la traçabilité.
- Permettre de filtrer le trafic.
- Les employés ne changent pas leur méthode de travail.
- Les employés non pas à connaitre les adresses IP des équipements cible mais seulement celui du serveur proxy ce qui nous offre une bonne sécurité.

Afin de visualiser un trafic dans un réseau (les interactions entre les utilisateurs et les ressources) et d'établir des droits d'accès qui vont contenir eux même des « commandes interdite », on va implémenter un proxy qui se situe entre les utilisateurs et les ressources, les utilisateurs devront donc passer par notre proxy qui va les rediriger vers les ressources cible, c'est ainsi que les accès vont être centraliser (tous passent par le proxy) et surveiller par l'auditeur.

Les spécifications de notre proxy seront les suivant :

- Ça sera un proxy sécurisé par le protocole SSH pour que les utilisateurs ne changent pas leurs méthodes de travail habituelles (utilisation d'un client SSH pour se connecter).
- Ce proxy va créer un fichier log qui contient les commandes envoyées par l'utilisateur vers la ressource ainsi que les réponses de la ressource envoyés vers l'utilisateur.
- Ce proxy va être relié avec une base de données qui va contenir les informations nécessaires pour déterminer si un utilisateur X a le droit d'accès à une ressource Y, et pour vérifier si l'utilisateur X peut exécuter une commande spécifique sur cette ressource ou non.

Pour faciliter la tâche de l'administrateur on a implémenté aussi une application web qui aura comme but de manipuler la base de données et permettre à l'auditeur de consulter les données des sessions et les fichiers logs.

Les opérations des administrateurs dans l'application web vont être stockées dans un fichier log que l'auditeur peut consulter par la suite.

3- Identification des acteurs

L'application est utilisée par 4 acteurs principaux :

- **L'auditeur** : c'est la personne qui utilise l'application pour effectuer les audits (consultation des logs).
- **L'administrateur** : c'est la personne responsable du bon fonctionnement de notre système et la gestion des différentes fonctionnalités.
- **L'utilisateur privilégié** : C'est la personne qui utilise les fonctionnalités de l'application pour se connecter aux ressources cibles.
- **Validateur :** C'est la personne responsable de la gestion des Administrateurs et la validation des autorisations.

4- Diagramme de cas d'utilisation générale

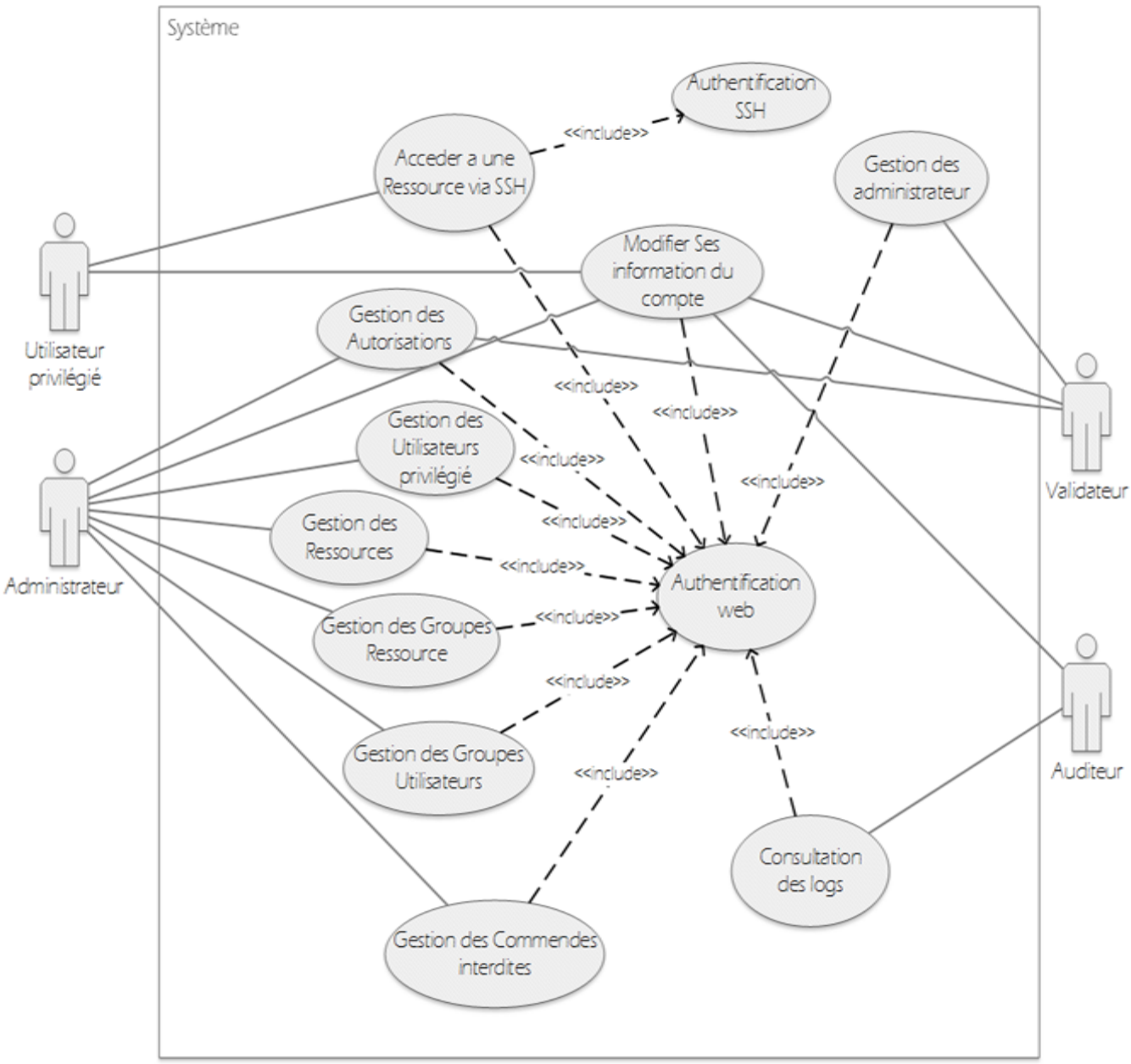


Figure 12 : Diagramme de cas d'utilisation générale.

5- Cas d'utilisation <<Accès à une ressource via SSH> >

L'utilisateur privilégié se connecte au proxy SSH et s'authentifie, il choisit par la suite l'une de ces ressources autorisées, ainsi le proxy authentifier l'utilisateur sur la ressource cible et il ouvre une session.

Le système crée un fichier log après la validation de l'authentification de l'utilisateur.

Le système enregistre et vérifie chaque commande envoyée par l'utilisateur.

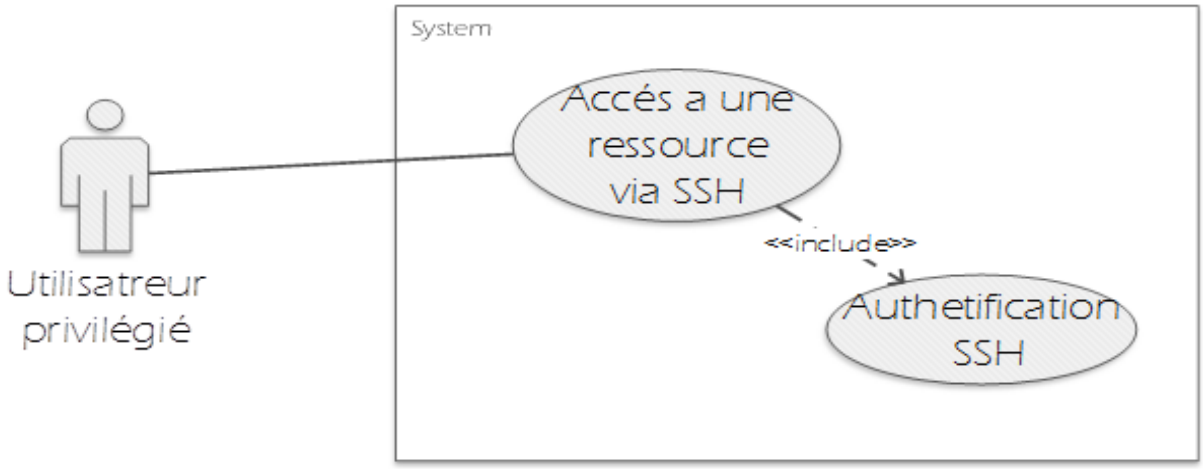


Figure 13 : Diagramme de cas d'utilisation << Démarrer une session >>

5.1- Description textuelle du cas d'utilisation <<accès à une ressource via SSH>>

Sommaire d'identification	
Titre	accès à une ressource via SSH
But	Administration des ressources
Résume	L'utilisateur doit s'authentifié et choisir la ressource cible puis une session de travail est ouverte par le système.
Acteur	Utilisateur privilégié

Description des enchainements	
Préconditions	Post conditions
- L'utilisateur possède un compte.	- ouverture de la session de travail.

Scenario : Accès à une ressource via SSH	
L'Utilisateur	Système
1 L'utilisateur se connecte au proxy via un client SSH comme Xshell.	**2** Le système demande à l'utilisateur de s'authentifier.

3 L'utilisateur envoi ces données d'authentifications. **5** L'utilisateur choisie une ressource.	**4** Le système vérifie l'authentification, crée un fichier log, et affiche les ressources cibles autorisées pour l'utilisateur. **6** Le système authentifie l'utilisateur sur la ressource cible et démarre une session. **7** Le système enregistre les métadonnées de la session dans la base des données. **8** Le système vérifie la commande, l'exécute et enregistre les commandes utilisées et la session dans fichier log.
Scenario alternative : commande interdite	
	8.a Le système vérifie la commande et envoie un message « Commande interdite » **9.a** Le système enregistre la session dans un fichier logs.
Scenario d'erreur	
E1 : Erreur d'authentification - Le système affiche un message d'erreur - Le scénario reprend au point 2	

5.2- Diagramme de séquence du cas d'utilisation<<Accès a une ressource via SSH>>

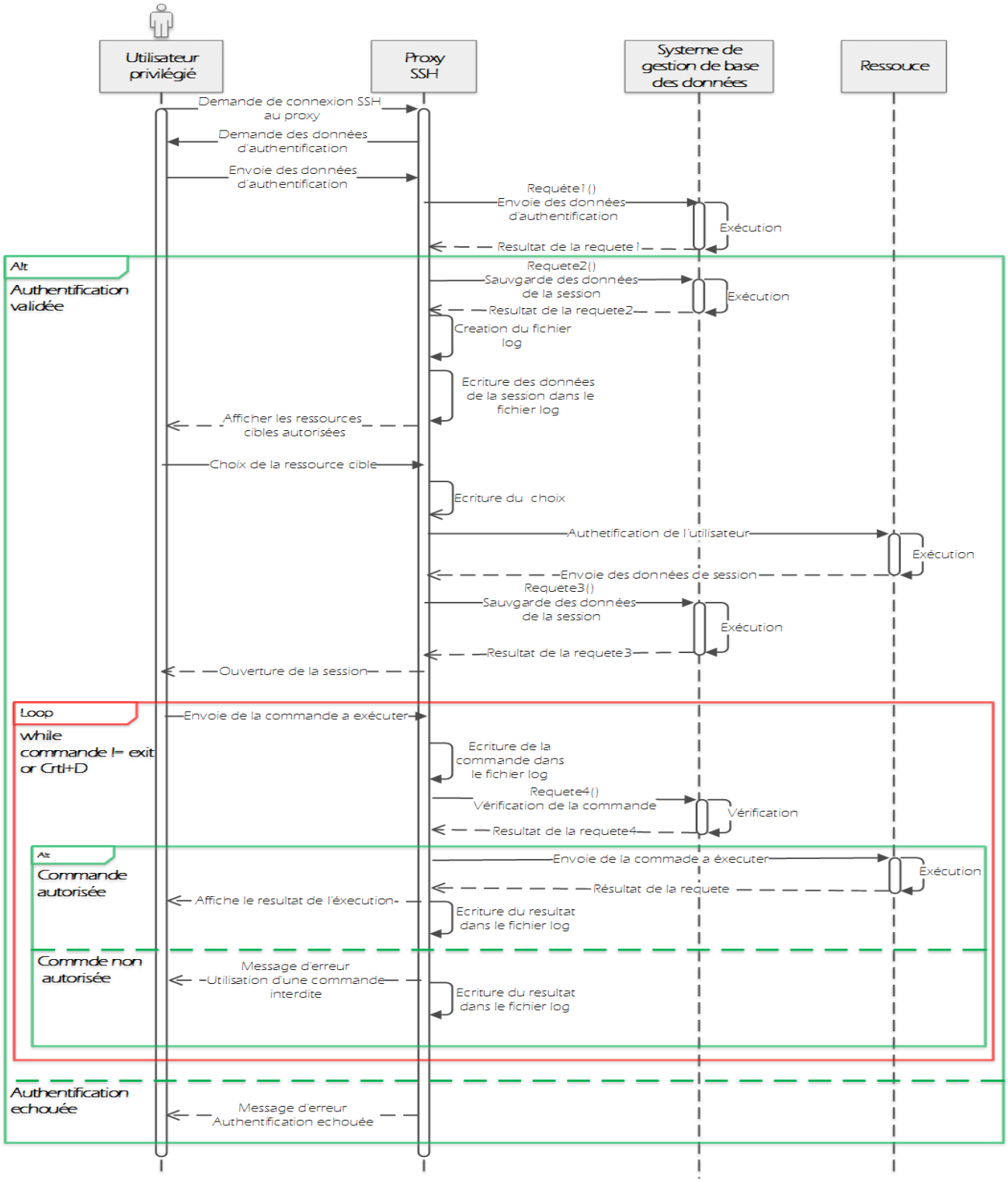


Figure 14 : Diagramme de séquence du cas d'utilisation << accès à une ressource via SSH >>

6- Cas d'utilisation <<Gestion des Utilisateurs Privilégiés>>

La gestion des utilisateurs privilégiés est l'une des tâches de l'administrateur, il peut exécuter les opérations suivantes : ajout, suppression, modification, recherche, l'affectation des listes de commande interdite et l'importation des utilisateurs.

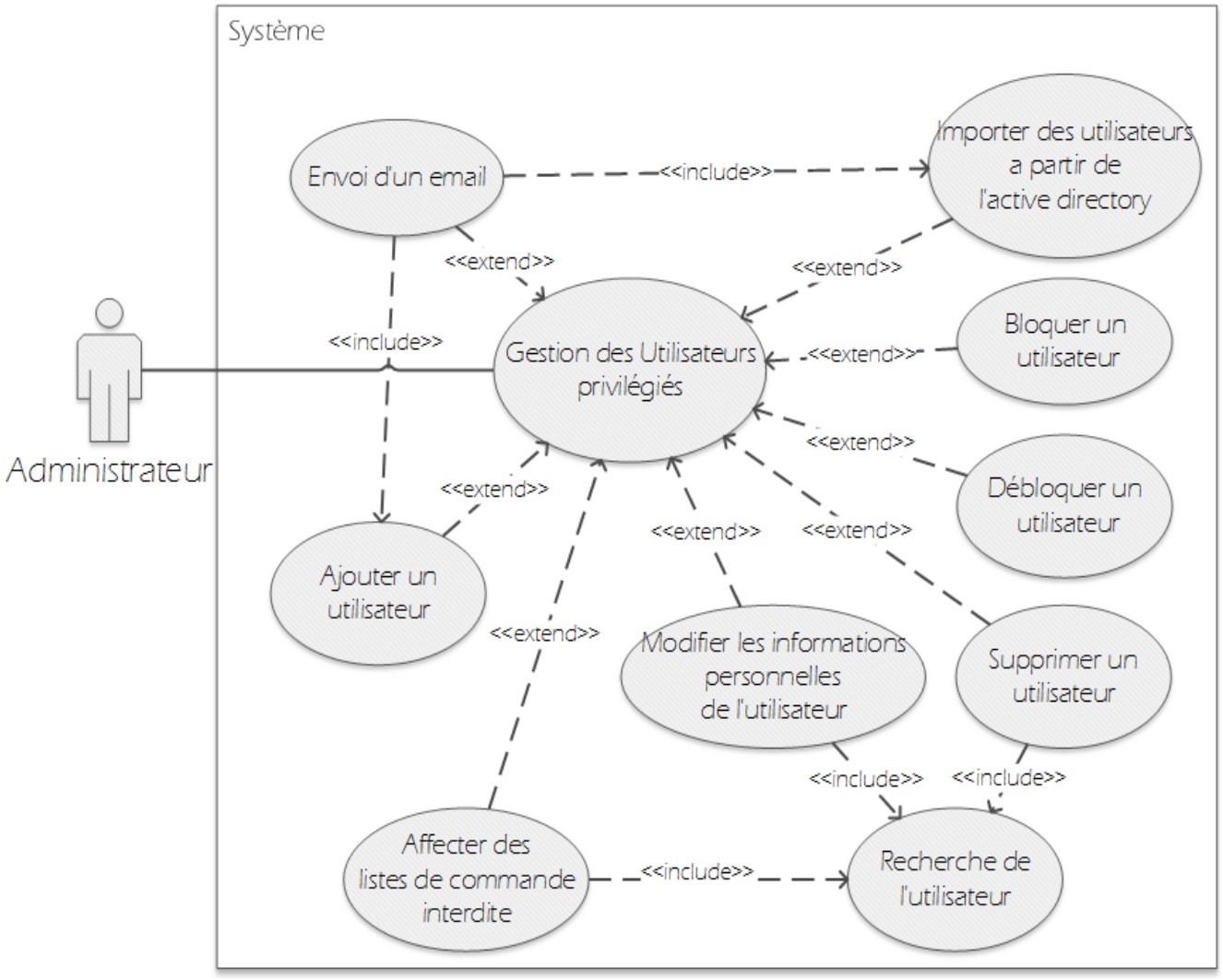


Figure 15 : Diagramme de cas d'utilisation << Gestion des utilisateurs privilégiés >>

6.1- Description textuelle du cas d'utilisation << Gestion des utilisateurs privilégiés >>

Sommaire d'identification

<table>
<tr><td>Titre</td><td colspan="2">Gestion des utilisateurs privilégiés.</td></tr>
<tr><td>But</td><td colspan="2">La gestion des utilisateur (ajout, modification, suppression, importation).</td></tr>
<tr><td>Résume</td><td colspan="2">Administrateur peut exécuter plusieurs opérations sur les utilisateurs de l’application comme l’ajout, suppression, modification, l’importation, blocage et déblocage.</td></tr>
<tr><td>Acteur</td><td colspan="2">Administrateur.</td></tr>
<tr><td colspan="3">Description des enchainements</td></tr>
<tr><td colspan="2">Préconditions</td><td>Post conditions</td></tr>
<tr><td colspan="2">- Administrateur est authentifié.
- L’administrateur à demander l’interface de gestion des utilisateurs</td><td>- Exécution des opérations de gestion.</td></tr>
<tr><td colspan="3">Scenario : Ajouter utilisateur</td></tr>
<tr><td colspan="2">User</td><td>Système</td></tr>
<tr><td colspan="2">1 L’administrateur choisie l’opération d’ajout d’utilisateur.
3 L’administrateur remplie le formulaire et valide l’opération.</td><td>2Le système affiche le formulaire d’ajout d’utilisateur.
4 Le système vérifie les champs du formulaire, exécute l’opération, renvoi un message de validation d’ajout de l’utilisateur et enregistre l’opération d’ajout dans le fichier log.
5 le système envoie un email à l’utilisateur ajouter.</td></tr>
<tr><td colspan="3">Scenario : Importer des utilisateurs à partir de l’active directory</td></tr>
</table>

1 L'administrateur choisie l'opération d'importation des utilisateurs à partir de l'active directory. **3** L'administrateur sélectionne les utilisateurs à importer et valide l'opération.	**2** Le système affiche l'interface d'importation d'utilisateurs. **4** Le système exécute l'opération, affiche un message de validation et enregistre l'opération d'importation dans le fichier log. **5** le système envoie un email aux utilisateurs ajouter.
Scenario : Modifier un utilisateur	
1 L'administrateur choisie l'opération de modification d'utilisateur. **3** L'administrateur remplie le formulaire et valide l'opération.	**2** Le système affiche le formulaire de modification utilisateur. **4** Le système vérifie les champs du formulaire, exécute l'opération, affiche un message de validation et enregistre l'opération de modification dans le fichier log.
Scenario : Supprimer un utilisateur	
1 L'administrateur choisie l'opération de suppression d'utilisateur. **3** L'administrateur confirme l'opération de suppression.	**2** Le système affiche l'interface de confirmation de la suppression. **4** Le système exécute l'opération, affiche un message de validation et enregistre l'opération de suppression dans le fichier log.
Scenario : Affecter des listes de commande interdite	
1 L'administrateur choisie l'opération d'affectation des listes de commande.	**2** Le système affiche l'interface de l'affectation des listes de commande.

3 L'administrateur sélectionne les listes de commande à affecter.	**4** Le système exécute l'opération, affiche un message de validation et enregistre l'opération d'affectation dans le fichier log.
Scenario d'erreur	
E1 : champs vides - le système renvoi un message d'erreur - le scenario ajouter utilisateur ou modifier utilisateur reprend au point 2 E2 : caractère non autorisé - le système renvoi un message d'erreur - le scenario ajouter utilisateur ou modifier utilisateur reprend au point 4 E3 : L'utilisateur existe dans la base des données - le système renvoi un message d'erreur - le scenario ajouter utilisateur reprend au point 4 E5 : impossible de ce connecté au serveur AD - Le système affiche un message d'erreur - Le scenario Importer des utilisateurs à partir de l'AD reprend au point 4	

6.2- Digramme de séquence du cas d'utilisation<< Gestion des Utilisateurs privilégiés >>

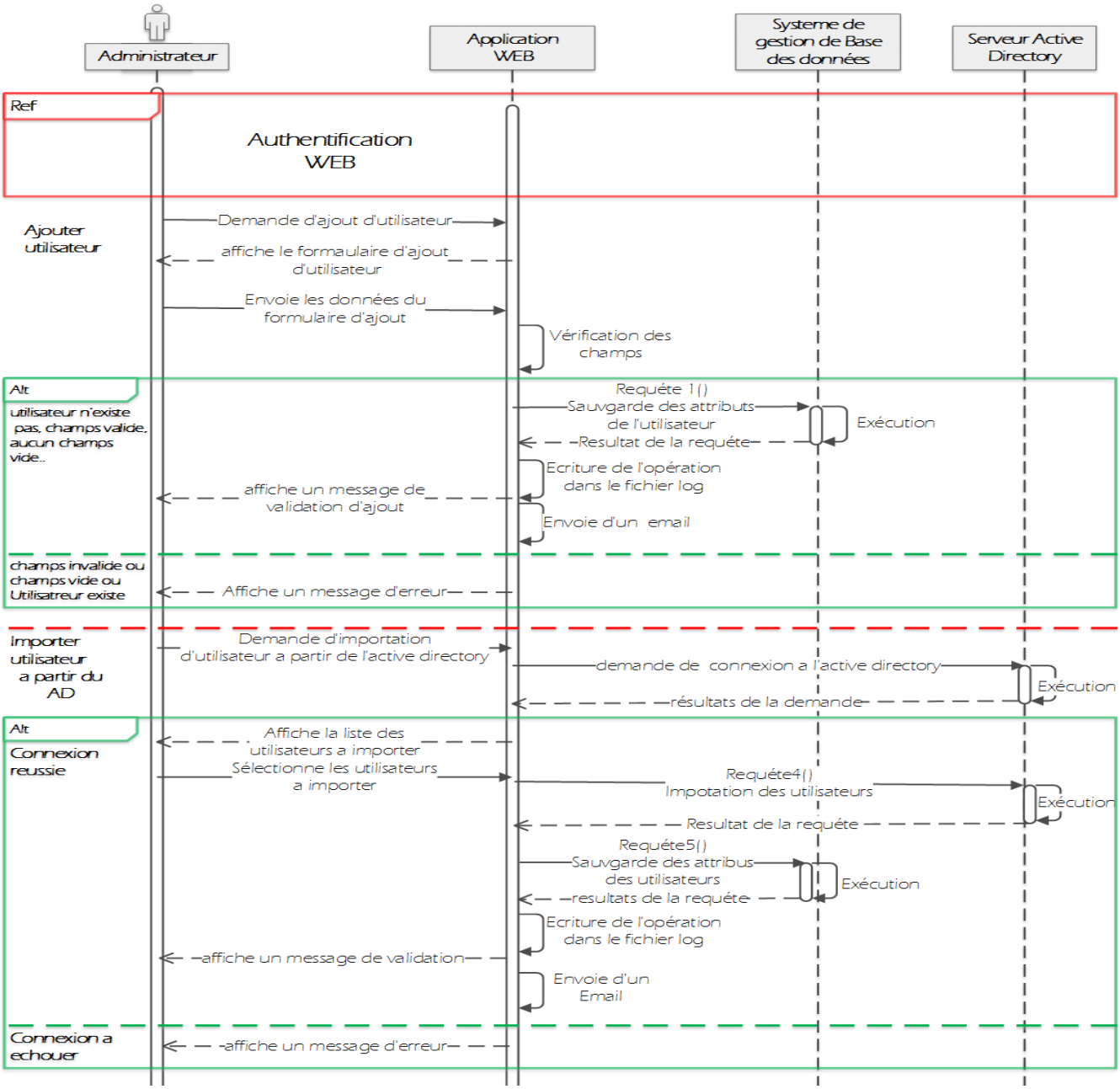
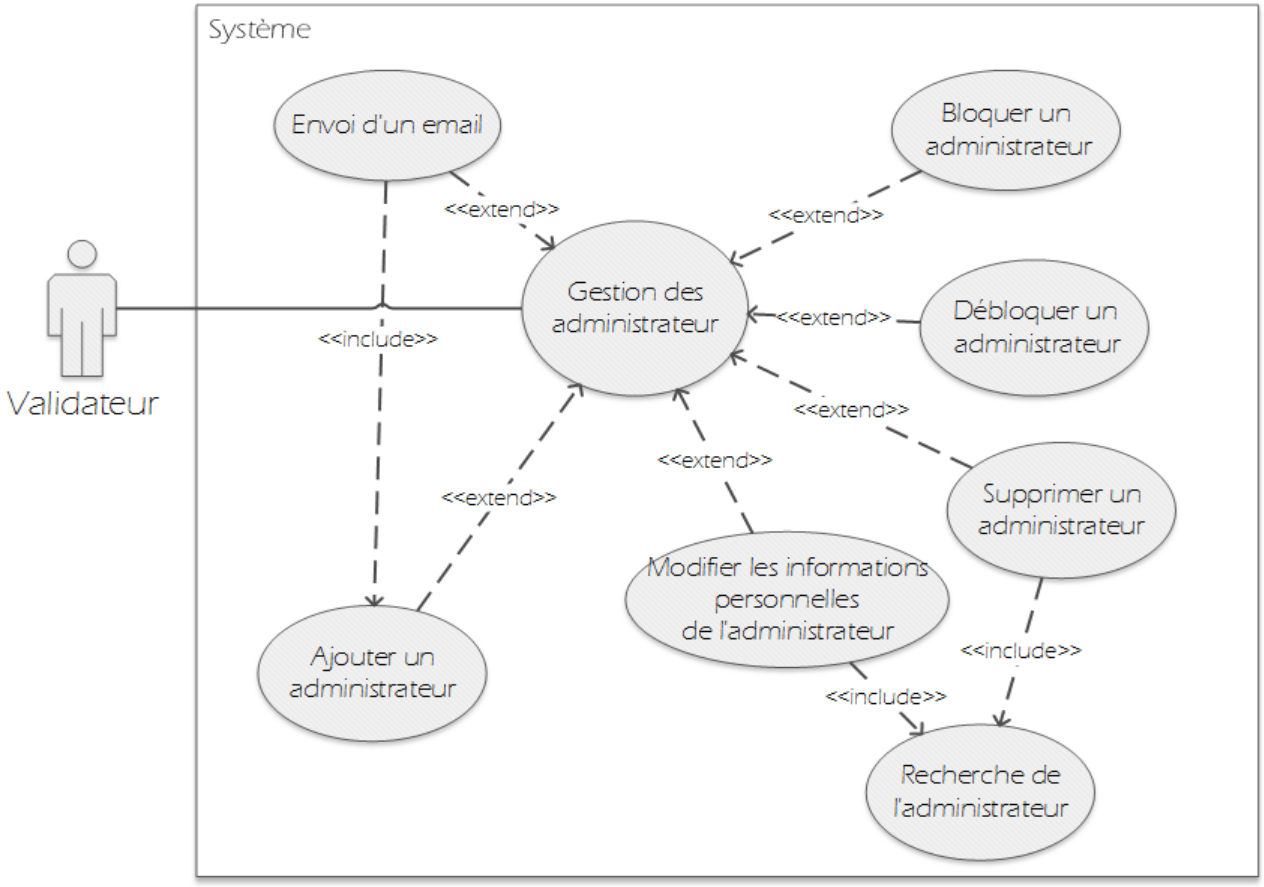


Figure 16 : Diagramme de séquence du cas d'utilisation << Gestion des utilisateurs privilégiés >>

7- Cas d'utilisation <<Gestion des Administrateurs>>

La gestion des administrateurs est l'une des tâches du validateur il peut exécuter les opérations suivantes : ajout, suppression, modification, l'importation, blocage, déblocage des administrateurs.



8- Cas d'utilisation <<Gestion des Ressources>>

La gestion des ressources est l'une des tâches de l'administrateur il peut exécuter les opérations suivantes : ajout, suppression, modification et l'importation des ressources.

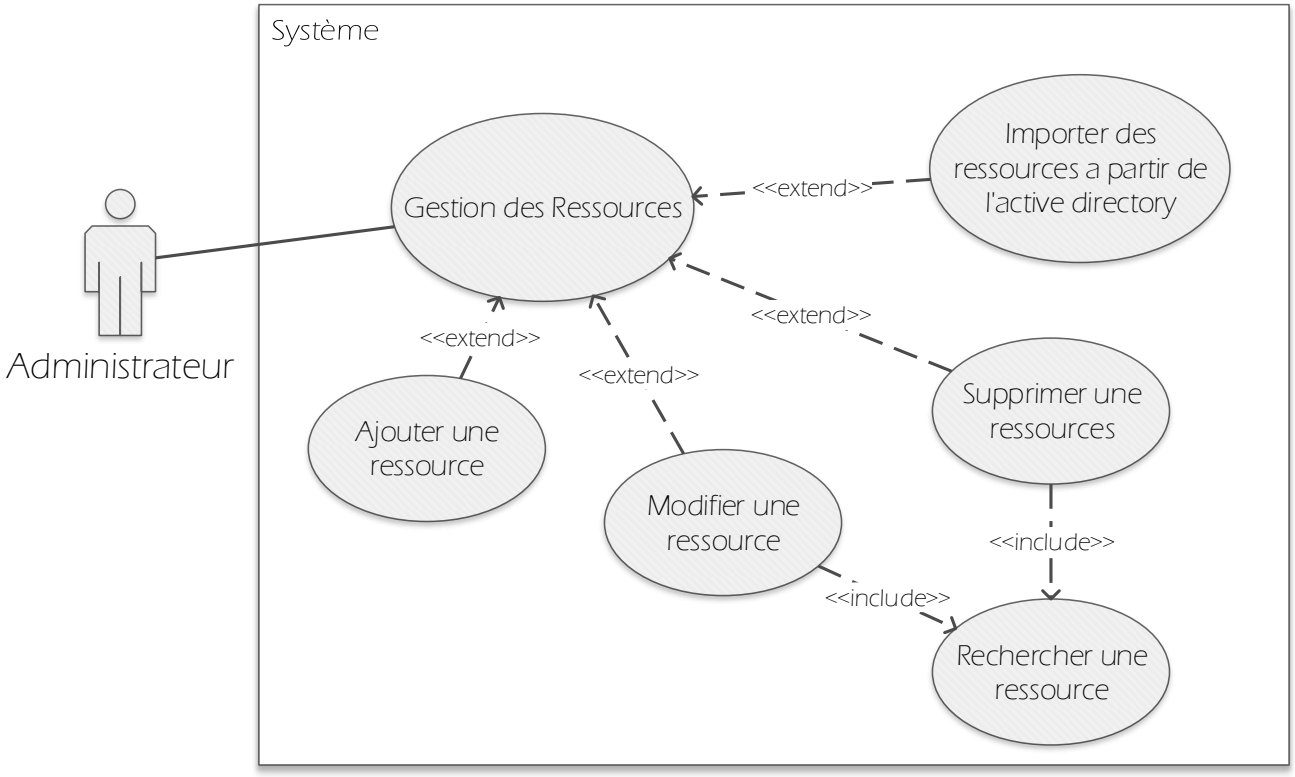


Figure 17 : Diagramme de cas d'utilisation << Gestion des ressources >>

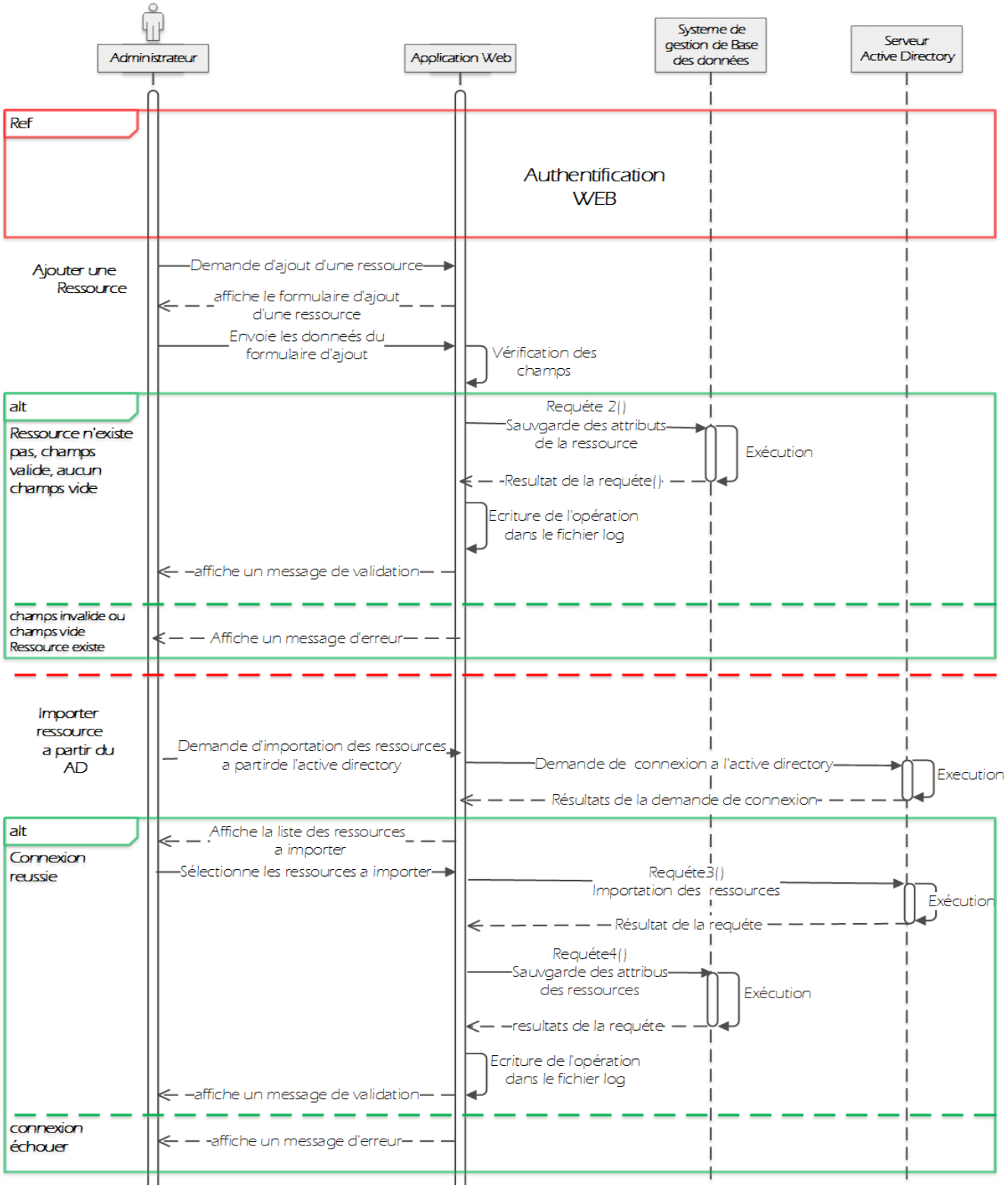
8.1- Description textuelle du cas d'utilisation << Gestion des ressources >>

Sommaire d'identification	
Titre	Gestion des ressources.
But	La gestion des ressources (ajout, modification, suppression, importation,).
Résume	Administrateur peut exécuter plusieurs opérations sur les utilisateurs de l'application comme l'ajout, suppression, modification et l'importation.
Acteur	Administrateur.
Description des enchainements	
Préconditions	Post conditions
- Administrateur est authentifié.	- Exécution des opérations de gestion.

- L'administrateur à demander l'interface de gestion des ressources.	
Scenario nominale	
User	Système
1 L'administrateur choisie l'opération d'ajout d'une ressource. **3** L'administrateur remplie le formulaire et valide l'opération.	**2** Le système affiche le formulaire d'ajout des ressources. **4** Le système vérifie les champs du formulaire, exécute l'opération, renvoi un message de validation et enregistre l'opération d'ajout dans le fichier log.
Scenario : Importer une ressource à partir de l'active directory	
1 L'administrateur choisie l'opération d'importation des ressources à partir de l'active directory. **3** L'administrateur sélectionne les ressources à importer et valide l'opération	**2** Le système affiche les ressources à importer. **4** Le système exécute l'opération, renvoi un message de validation et enregistre les ressources importer dans le fichier log.
Scenario : Modifier une ressource	
1 L'administrateur choisie l'opération de modification de la ressource. **3** L'administrateur remplie le formulaire et valide l'opération.	**2**Le système affiche le formulaire de modification des ressources. **4** Le système vérifie les champs du formulaire, exécute l'opération, renvoi un message de validation et enregistre l'opération de modification dans le fichier log.
Scenario : Supprimer une ressource	

1 L'administrateur choisie l'opération de suppression de la ressource. **3** L'administrateur valide l'opération. .	**2** Le système affiche l'interface de confirmation de la suppression. **4** Le système exécute l'opération, renvoi un message de validation et enregistre l'opération de suppression dans le fichier log.
Scenario d'erreur	
E1 : champs vides - Le système renvoi un message d'erreur. - Le scenario ajouter ressource ou modifier ressource reprend au point 4 E2 : caractère non autorisé - Le système renvoi un message d'erreur. - Le scenario ajouter ressource ou modifier ressource reprend au point 4 E3 : La ressource existe dans la base des données - Le système renvoi un message d'erreur. - Le scenario ajouter ressource reprend au point 4. - Le scenario importer ressource reprend au point 2. E4 : connexion à échouer - Le système affiche un message d'erreur. - Le scenario importation des ressources à partir de l'AD reprend au point 1.	

8.2- Diagramme de séquence du cas d'utilisation<<gestion des ressources>>



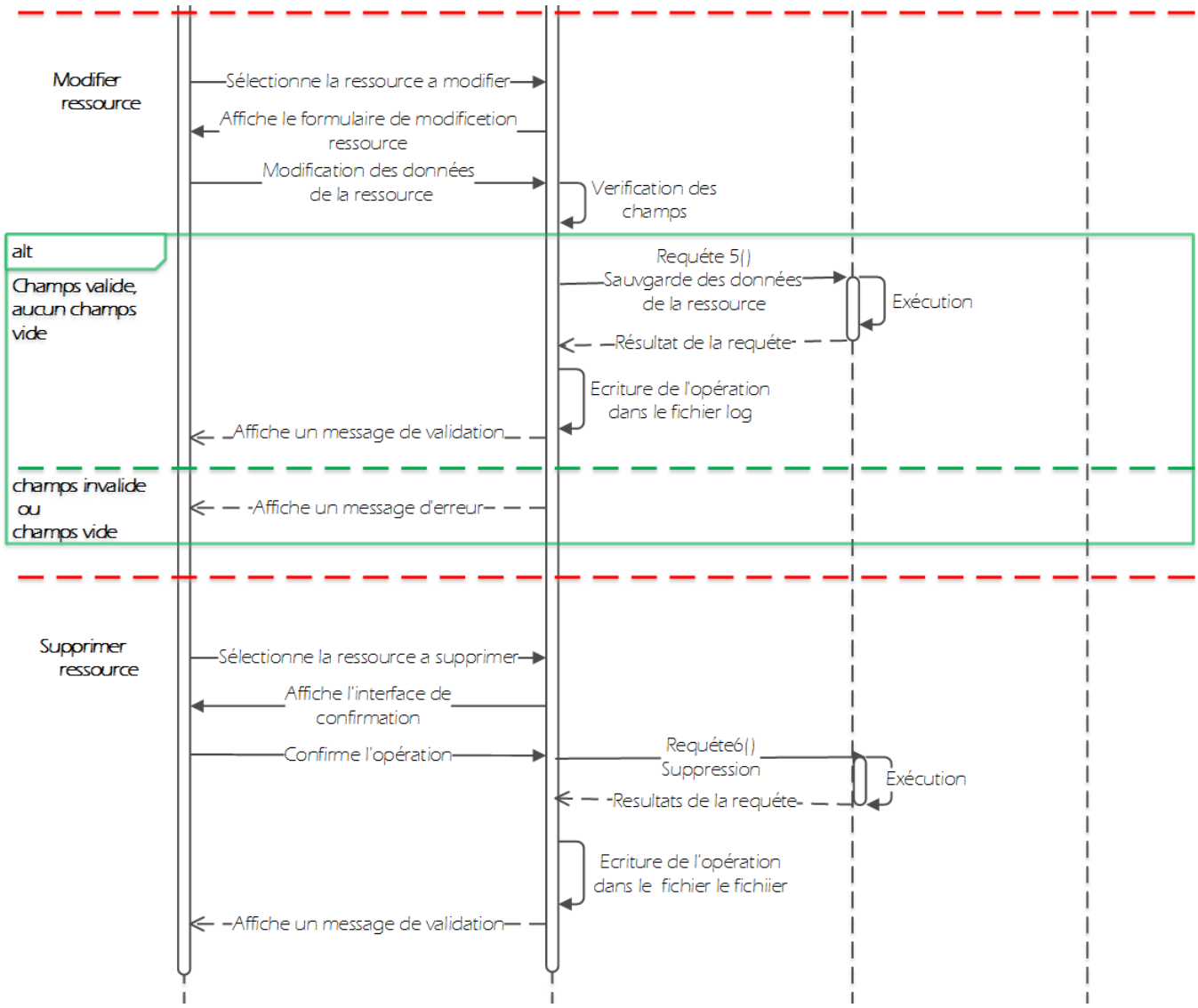


Figure 18 : Diagramme de séquence du cas d'utilisation << Gestion des ressources >>

9- Cas d'utilisation <<Gestion des groupes des utilisateurs privilégiés >>

La gestion des groupes de utilisateurs est l'une des tâches de l'administrateur il peut exécuter les opérations suivantes : ajouter un groupe et, suppression groupe et utilisateur, l'affichage des ressources autorisées.

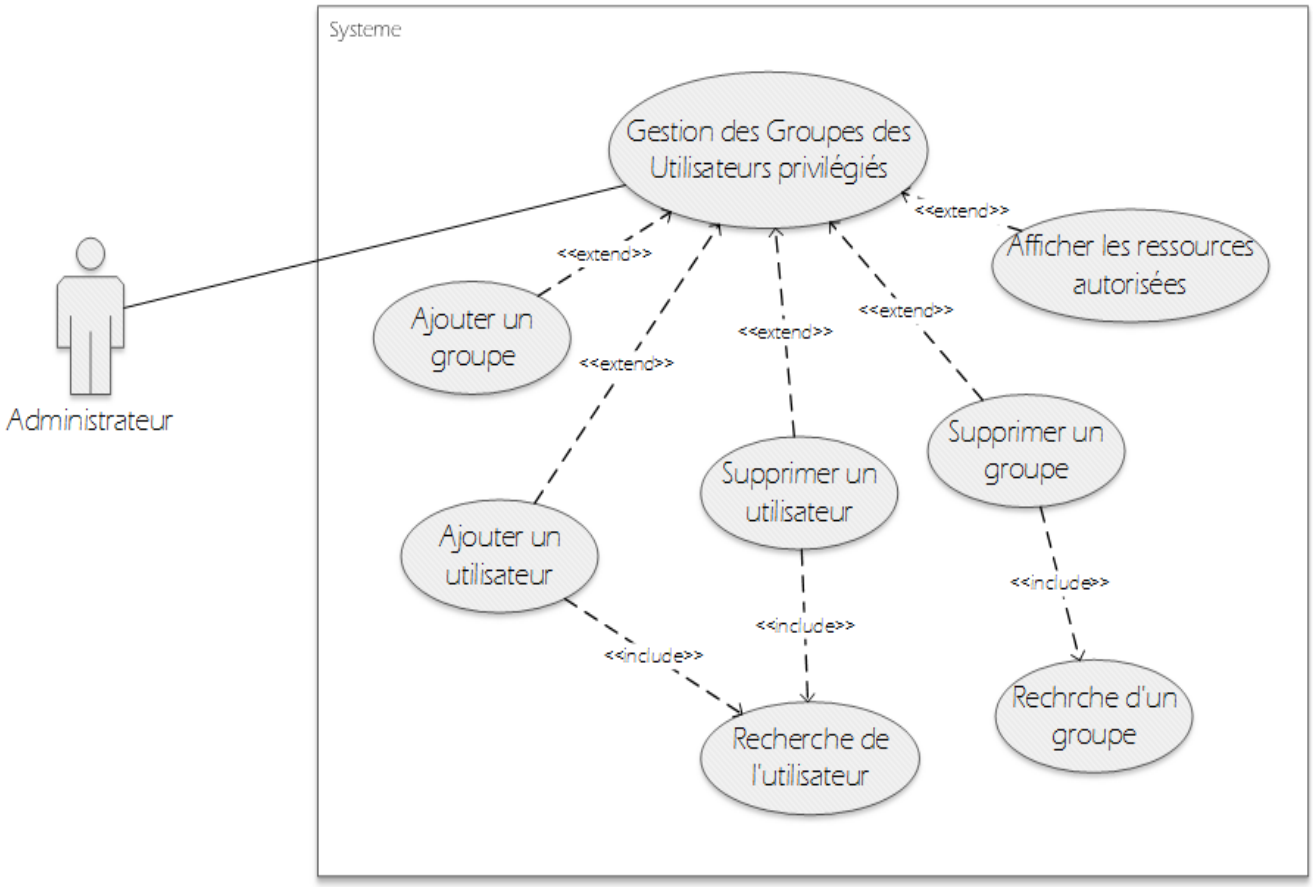


Figure 19 : Diagramme de cas d'utilisation << Gestion des groupes des utilisateurs >>

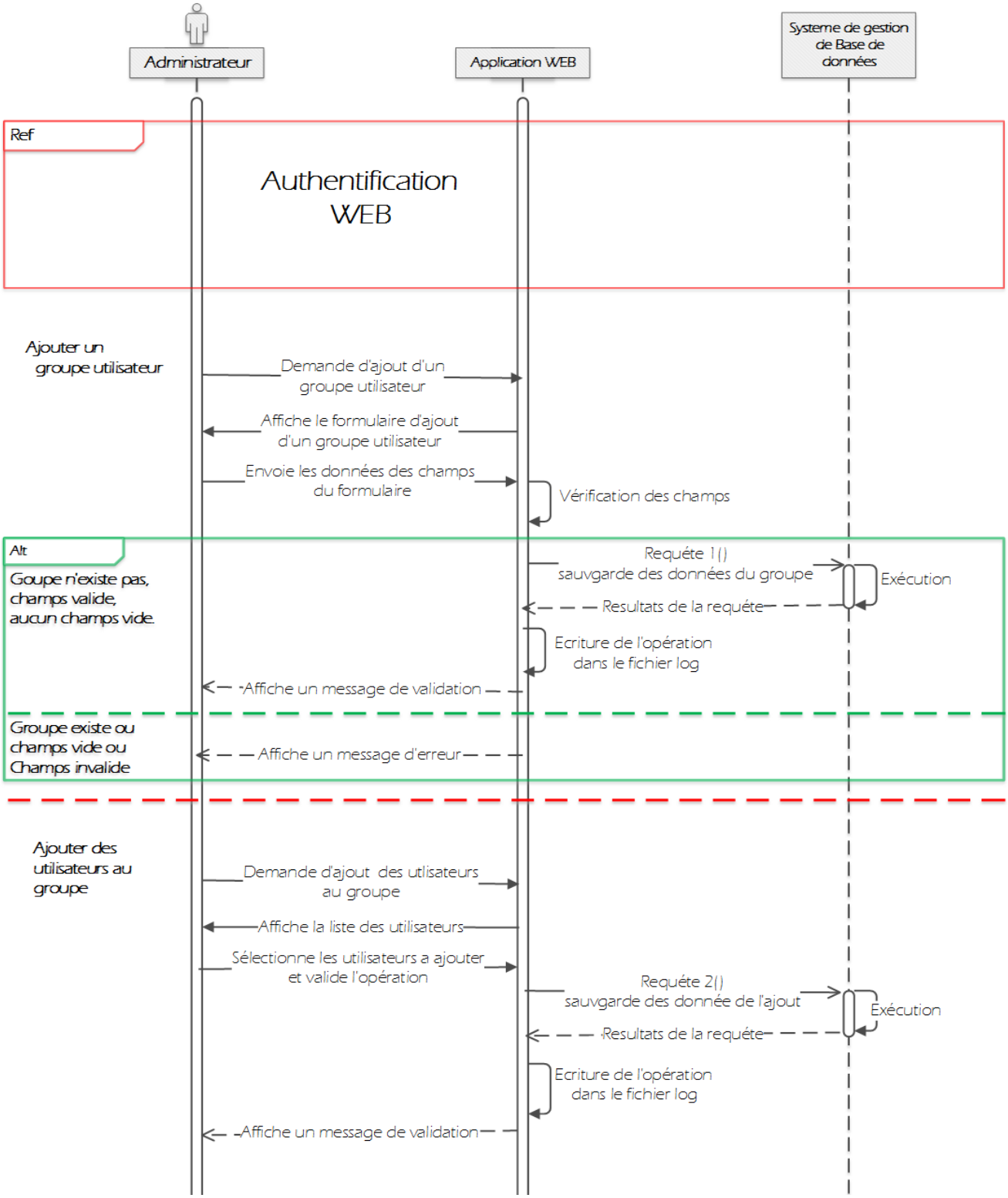
9.1- Description textuelle du cas d'utilisation << Gestion des Groupes des utilisateurs privilégiés >>

Sommaire d'identification	
Titre	Gestion des groupes des utilisateurs privilégiés
But	Gestion des groupes des utilisateurs pour faciliter et optimiser l'attribution des permissions

<table>
<tr><td>Résume</td><td colspan="2">L’administrateur peut gérer et créés les groupes des utilisateurs en utilisent les opérations d’ajout, modification, suppression, en plus l’administrateur peut consulter les ressources autorisées du groupe.</td></tr>
<tr><td>Acteur</td><td colspan="2">Administrateur</td></tr>
<tr><td colspan="3">Description des enchainements</td></tr>
<tr><td colspan="2">Préconditions</td><td>Post conditions</td></tr>
<tr><td colspan="2">- Administrateur et authentifié.
- L’administrateur à demander l’interface de gestion des groupes des utilisateurs</td><td>- la gestion des groupes des utilisateurs</td></tr>
<tr><td colspan="3">Scenario : Ajouter un groupe</td></tr>
<tr><td colspan="2">User</td><td>Système</td></tr>
<tr><td colspan="2">1 L’administrateur choisie l’opération Ajouter un groupe.
3L’administrateur remplie le formulaire et valide l’opération</td><td>2 Le système affiche le formulaire d’ajout de groupe.
5 Le système vérifie les champs du formulaire, exécute l’opération, renvoi un message de validation et enregistre l’opération d’ajout dans le fichier log.</td></tr>
<tr><td colspan="3">Scenario : Ajouter des utilisateurs au groupe</td></tr>
<tr><td colspan="2">1 l’administrateur choisie l’opération ajouter des utilisateurs au groupe.
3 l’administrateur sélectionne les utilisateurs à ajouter et valide l’opération.</td><td>2 Le système affiche la liste des utilisateurs qui n’existe pas dans le groupe.
5 Le système exécute l’opération, renvoi un message de validation et enregistre l’opération de l’ajout dans le fichier log.</td></tr>
<tr><td colspan="3">Scenario : Supprimer un utilisateur d’un groupe</td></tr>
<tr><td colspan="2">1 L’administrateur choisie l’opération supprimer un utilisateur d’un groupe.
3 L’administrateur valide l’opération.</td><td>2 Le système affiche l’interface de confirmation de la suppression.</td></tr>
</table>

	5 Le système exécute l'opération, renvoi un message de validation et enregistre l'opération de suppression dans le fichier log.
Scenario : Supprimer un groupe	
1 l'administrateur choisie l'opération supprimer un groupe. **3** L'administrateur valide l'opération.	**2** Le système affiche l'interface de confirmation de la suppression. **4** Le système exécute l'opération, renvoi un message de validation et enregistre l'opération de suppression dans le fichier log.
Scenario: afficher les ressource autorisés	
1 L'administrateur choisie l'opération afficher les ressources autorisées.	**2** Le système affiche les ressources autorisées.
Scenario d'erreur	
E1 : champs vides - Le système renvoi un message d'erreur - Le scenario ajouter un groupe reprend au point 2 E2 : caractère non autorisé - Le système renvoi un message d'erreur - Le scenario ajouter un groupe reprend au point 2 E3 : La groupe existe dans la base des données - Le système renvoi un message d'erreur - Le scenario ajouter un groupe reprend au point 2	

9.2- Diagramme de séquence du cas d'utilisation <<gestion des groupes utilisateurs privilégiés>>



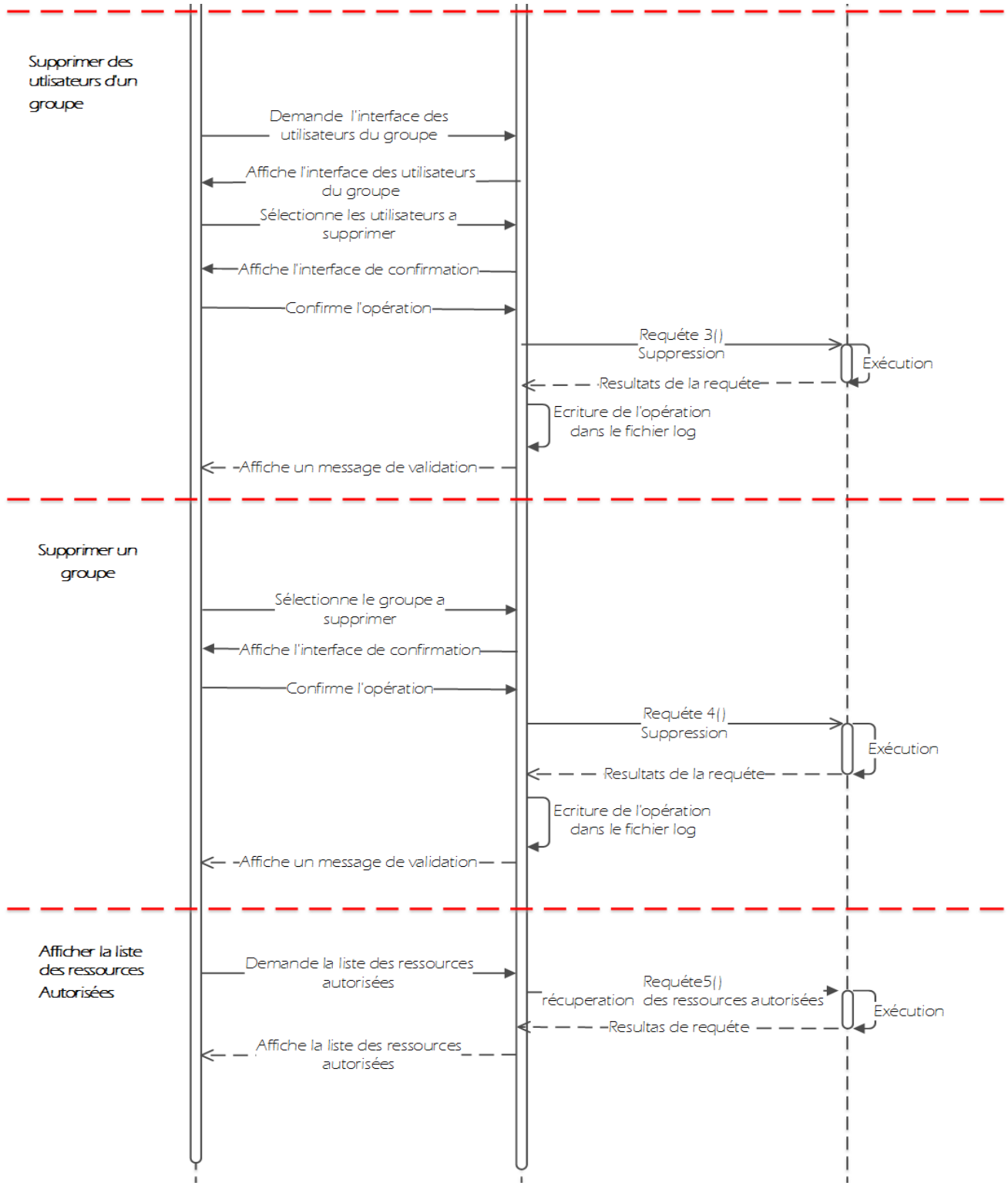


Figure 20 : Diagramme de séquence du cas d'utilisation << Gestion des groupe utilisateur >>

10- Cas d'utilisation <<Gestion des groupes des ressources >>

La gestion des groupes de ressources est l'une des tâches de l'administrateur il peut exécuter les opérations suivantes :

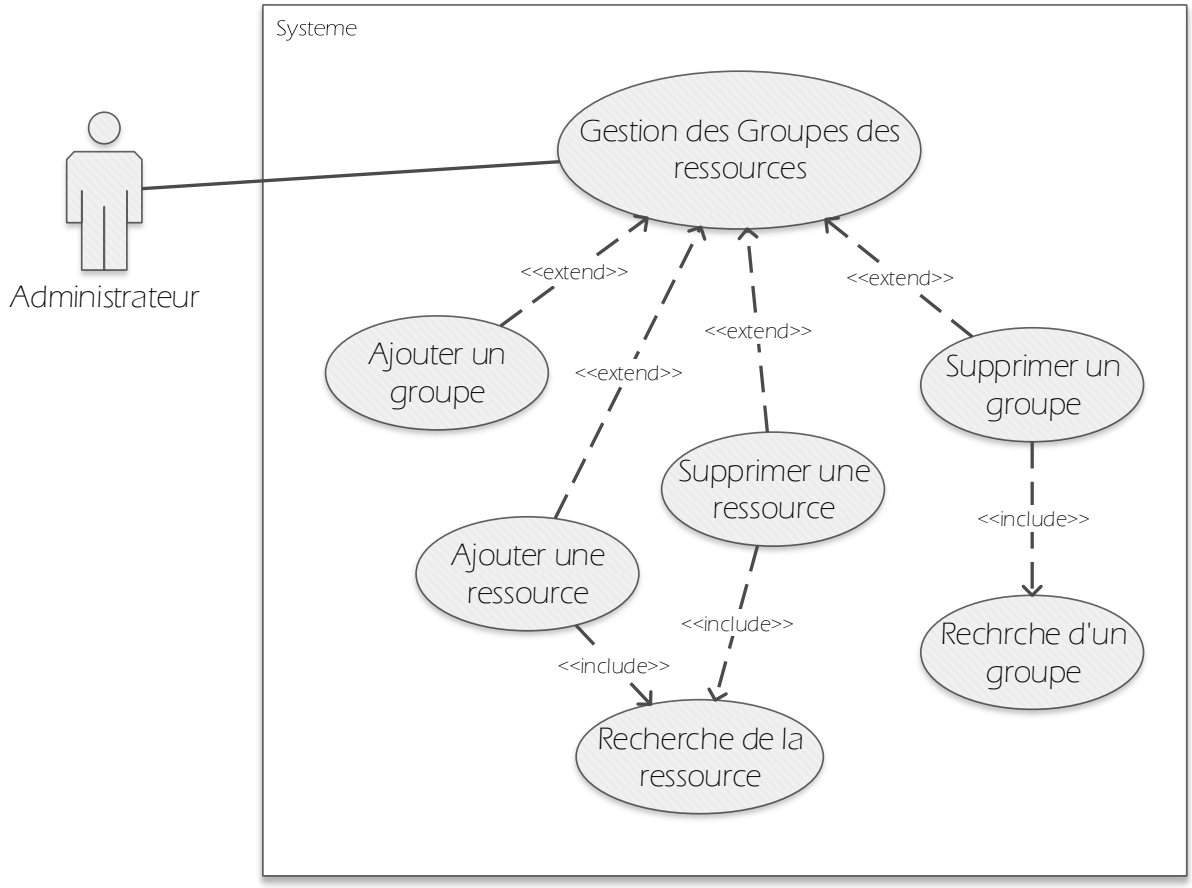


Figure 21 : Diagramme de cas d'utilisation << Gestion des groupes des ressources >>

10.1- Description textuelle du cas d'utilisation << Gestion des groupes des Ressources>>

Sommaire d'identification	
Titre	Gestion des groupes des ressources

But	Gestion des groupes des ressources pour faciliter et optimiser l'attribution des permissions
Résume	L'administrateur peut gérer les groupes des ressources en utilisent les opérations d'ajout, modification et suppression.
Acteur	Administrateur

Description des enchainements	
Préconditions	Post conditions
- Administrateur et authentifié. - L'administrateur à demander l'interface de gestion des groupes des ressources.	- la gestion des groupes des ressources

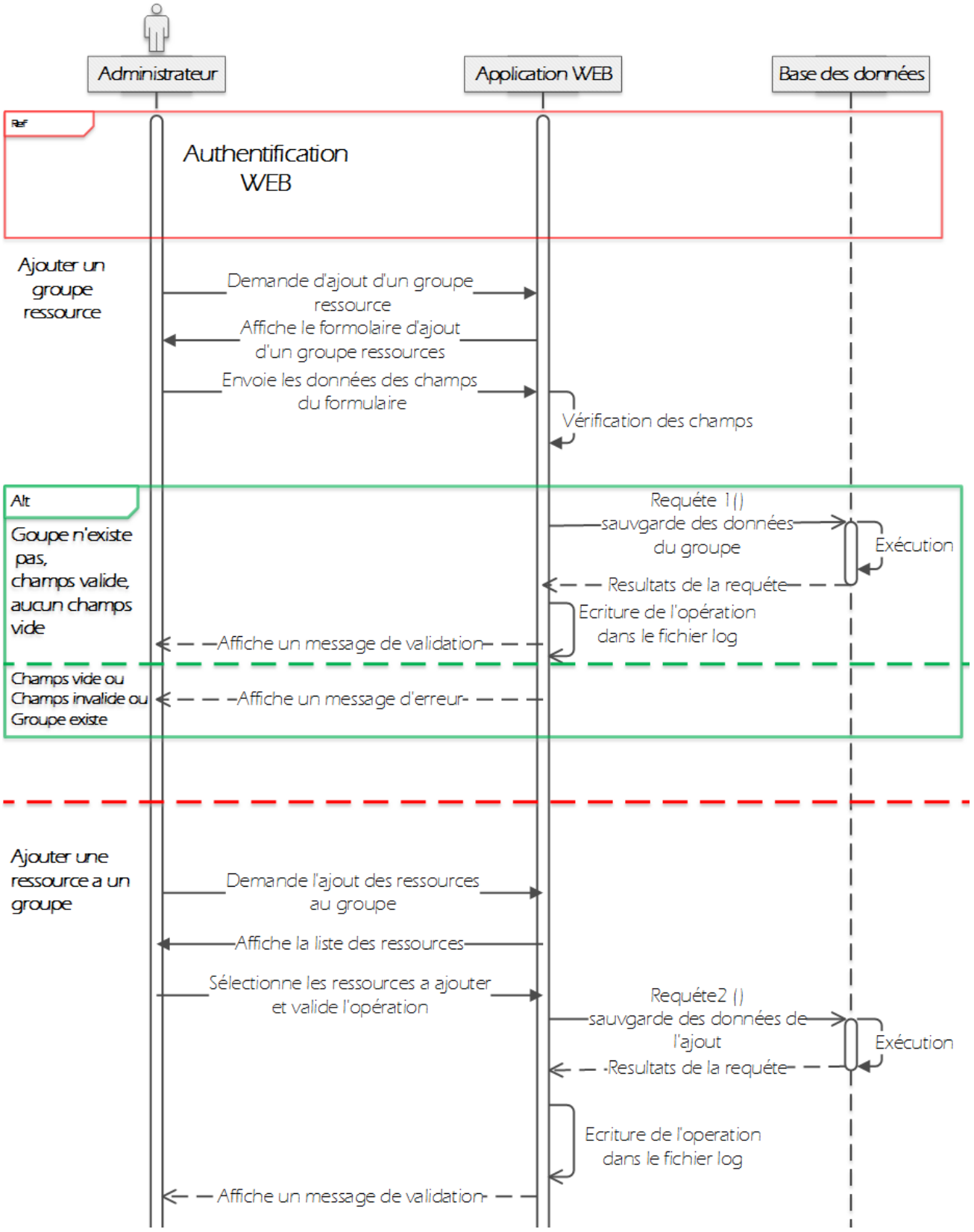
Scenario	
User	Système
1 l'administrateur choisie l'opération ajouter un groupe. **3** L'administrateur remplie le formulaire et valide l'opération.	**2** le système affiche l'interface d'ajout groupe. **4** Le système vérifie les champs du formulaire, exécute l'opération, renvoi un message de validation et enregistre l'opération d'ajout dans le fichier log.

Scenario : Ajouter des ressources a un groupe	
1 l'administrateur choisie l'opération ajouter des ressources a un groupe. **3** l'administrateur sélectionne les ressources à ajouter et valide l'opération.	**2** Le système affiche la liste des ressources qui n'existe pas dans le groupe. **4** Le système exécute l'opération, renvoi un message de validation et enregistre l'opération d'ajout dans le fichier log.

Scenario : Supprimer une ressources d'un groupe	
1 l'administrateur choisie l'opération supprimer une ressource d'un groupe.	**2** Le système affiche l'interface de confirmation de la suppression.

3 L'administrateur valide l'opération.	**4** Le système exécute l'opération, renvoi un message de validation et enregistre l'opération de suppression dans le fichier log.
Scenario : Supprimer un groupe	
1 L'administrateur choisie l'opération supprimer un groupe. **3** L'administrateur valide l'opération.	**2** Le système affiche l'interface de confirmation de la suppression. **4** Le système exécute l'opération, renvoi un message de validation et enregistre l'opération de suppression dans le fichier log.
Scenario d'erreur	
E1 : champs vides - Le système renvoi un message d'erreur - Le scenario ajouter un groupe reprend au point 2 E2 : caractère non autorisé - Le système ajouter un groupe renvoi un message d'erreur - Le scenario reprend au point 2 E3 : La groupe existe dans la base des données - Le système renvoi un message d'erreur - Le scenario ajouter un groupe reprend au point 2	

10.2- Diagramme de séquence du cas d'utilisation<< gestion des groupes ressources >>


Administrateur
Application WEB
Base des données
Ref
Authentification WEB
Ajouter un groupe ressource
Demande d'ajout d'un groupe ressource
Affiche le formolaire d'ajout d'un groupe ressources
Envoie les données des champs du formulaire
Vérification des champs
Alt
Goupe n'existe pas, champs valide, aucun champs vide
Requéte 1() sauvgarde des données du groupe
Exécution
Resultats de la requéte
Ecriture de l'opération dans le fichier log
Affiche un message de validation
Champs vide ou Champs invalide ou Groupe existe
Affiche un message d'erreur
Ajouter une ressource a un groupe
Demande l'ajout des ressources au groupe
Affiche la liste des ressources
Sélectionne les ressources a ajouter et valide l'opération
Requéte2 () sauvgarde des données de l'ajout
Exécution
Resultats de la requéte
Ecriture de l'operation dans le fichier log
Affiche un message de validation

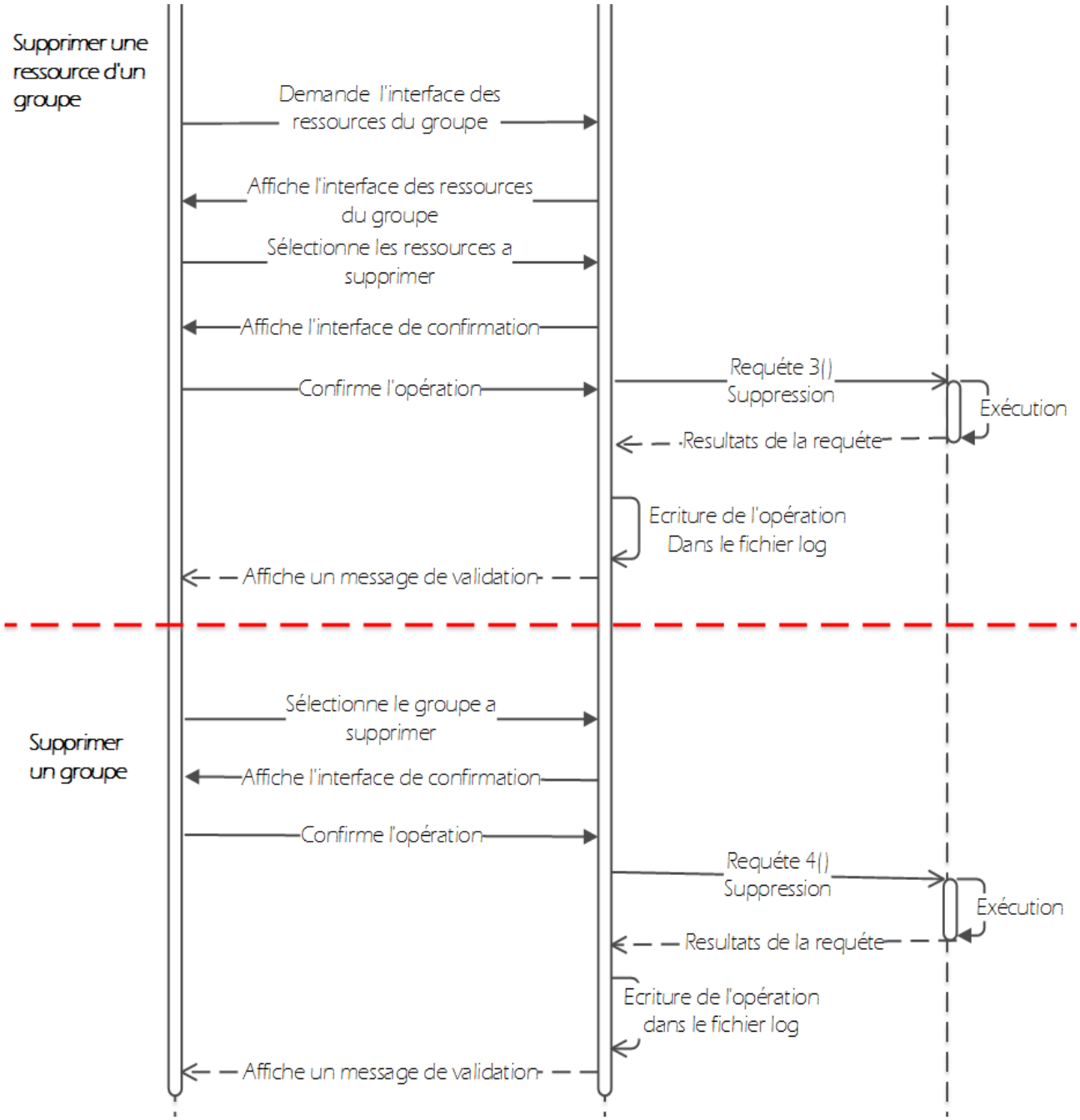


Figure 22 : Diagramme de séquence du cas d'utilisation << Gestion des groupes des ressources >>

11- Cas d'utilisation <<Gestion des Autorisations>>

La gestion des Autorisations est divisée entre deux acteurs :

- **Administrateur :** il peut exécuter les opérations suivantes : ajout et suppression, mais l'ajout d'une nouvelle autorisation doit être valider par un validateur.

- **Validateur :** Son rôle est de valider l'ajout des autorisations.

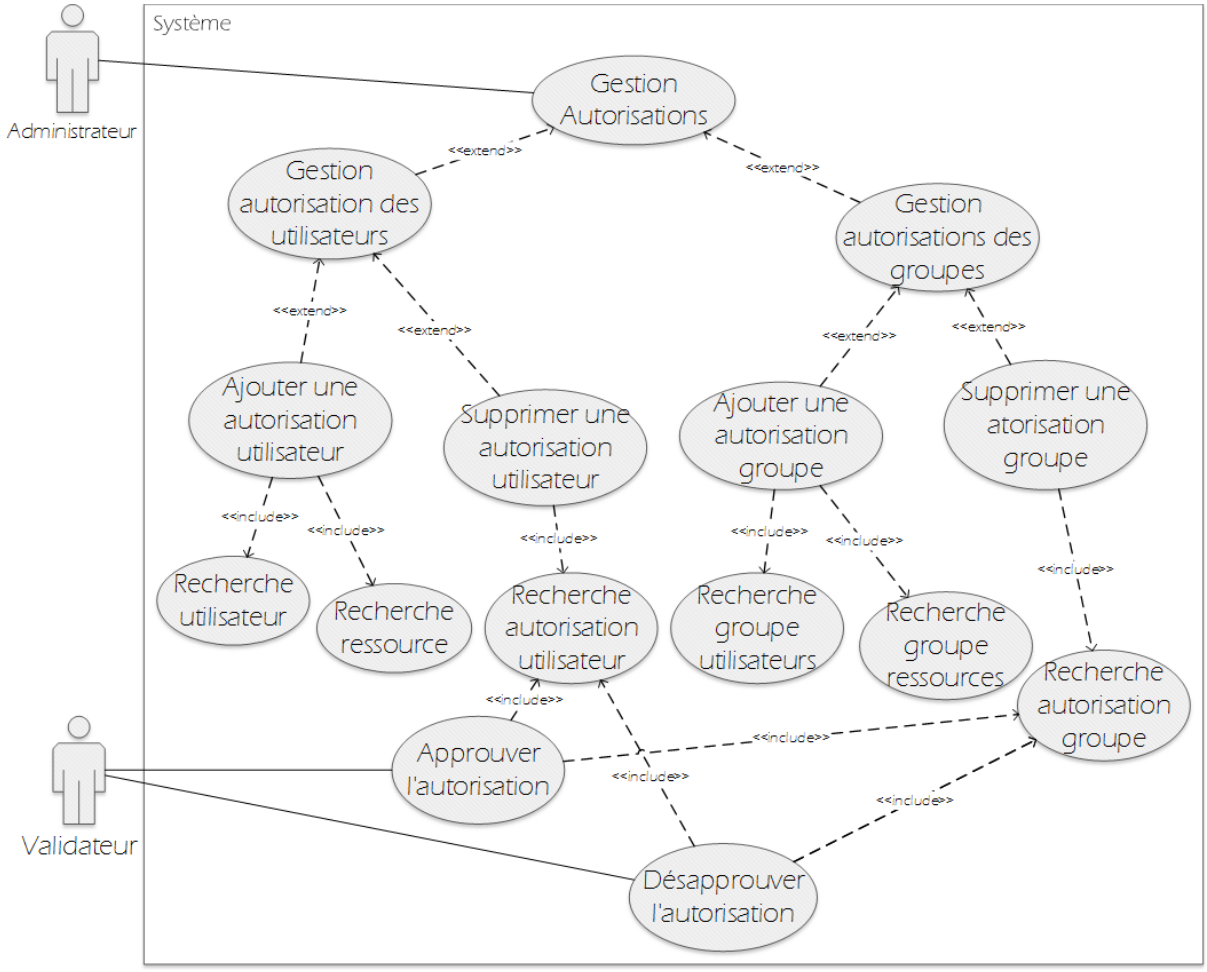


Figure 23 : Diagramme de cas d'utilisation << gestion des Autorisation>>

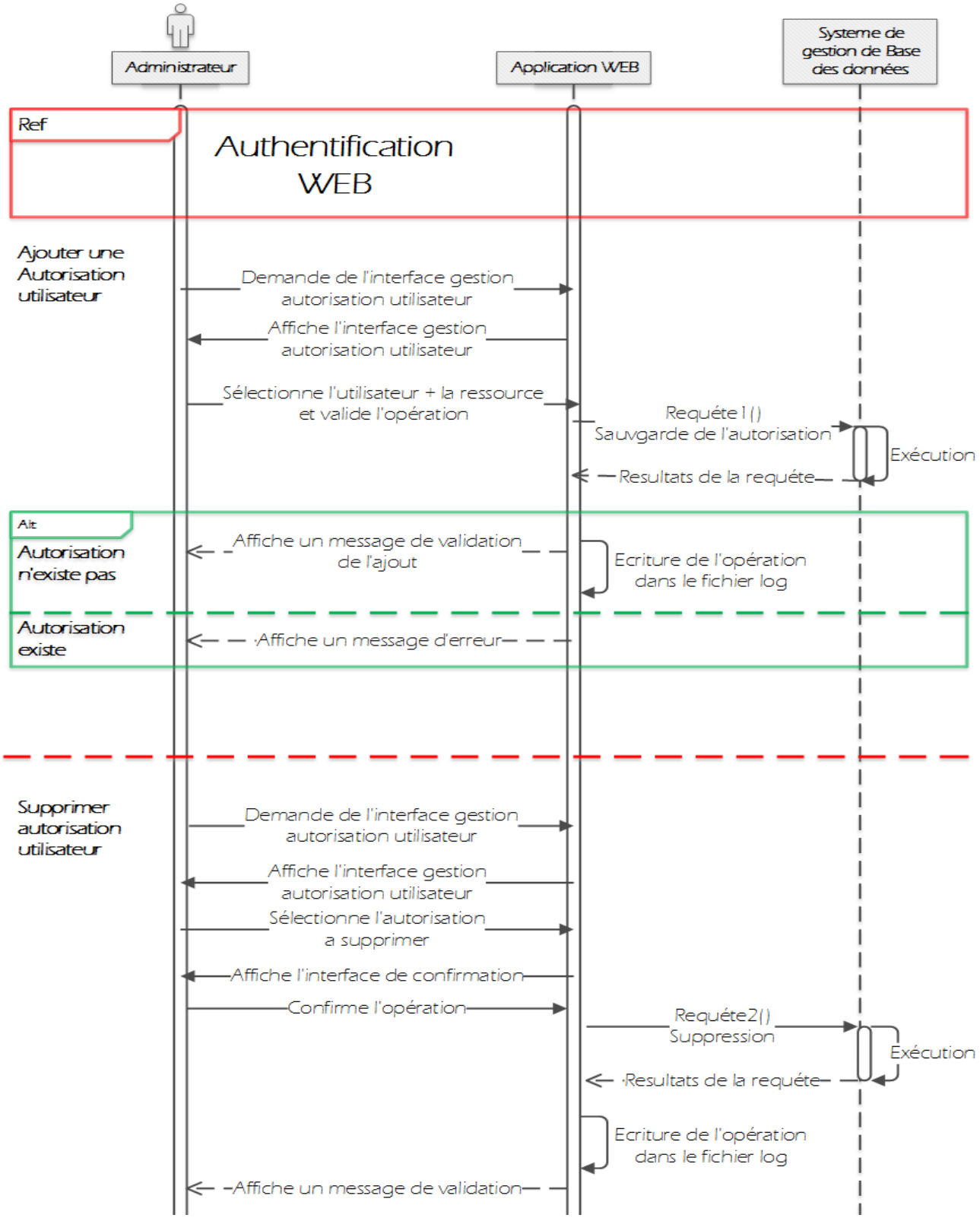
11.1- Description textuelle du cas d'utilisation << Gestion des Autorisation >>

Sommaire d'identification	
Titre	Gestion des autorisations
But	Définir la liste des ressources autorisées pour un/des utilisateur(s)
Résume	L'administrateur peut gérer les autorisations d'accès des utilisateurs aux ressources utilisent les opérations d'ajout et suppression. Le validateur valide l'ajout de l'autorisation
Acteur	Administrateur , validateur

Description des enchainements	
Préconditions	Post conditions
- Administrateur et authentifié.	- la gestion des autorisations
Scenario : ajouter une autorisation utilisateur	
User	Système
1 L'administrateur demande l'interface gestion autorisation utilisateur. **3** L'administrateur sélectionne l'utilisateur et la ressource et valide l'ajout de l'autorisation.	**2** Le système affiche l'interface gestion autorisation utilisateur. **5** le système exécute l'opération, affiche un message de validation et enregistre l'opération d'ajout dans le fichier log. **6** Le système envoie un email au validateur.
Scenario : Supprimer une autorisation utilisateur	
1 L'administrateur demande l'interface gestion autorisation utilisateur. **3** l'administrateur choisie l'opération de suppression. **5** L'administrateur valide l'opération.	**2** Le système affiche l'interface gestion autorisation utilisateur. **4** Le système affiche l'interface de confirmation de la suppression. **6** Le système exécute l'opération, affiche un message de validation et enregistre l'opération de suppression dans le fichier log.
Scenario : Ajouter une autorisation groupe	
1 L'administrateur demande l'interface gestion autorisation des groupes. **3** L'administrateur sélectionne le groupe utilisateurs et le groupe ressources et valide l'ajout de l'autorisation	**2** Le système affiche l'interface gestion autorisation des groupes. **4** Le système exécute l'opération, affiche un message de validation et enregistre l'opération d'ajout dans le fichier log. **5** Le système envoie un email au validateur. L'opération de d'ajout dans le fichier log.

	6 Le système envoie un email au validateur.
Scenario : Supprimer une autorisation des groupe	
1 L'administrateur demande l'interface gestion autorisation des groupes. **3** l'administrateur choisie l'opération de suppression. **5.c** L'administrateur valide l'opération.	**2** Le système affiche l'interface gestion autorisation des groupes. **4** Le système affiche l'interface de confirmation de la suppression. **6** Le système exécute l'opération, affiche un message de validation et enregistre l'opération de suppression dans le fichier log.
Scenario : Valider les autorisation utilisateur	
1 Le validateur demande l'interface de gestion autorisation utilisateurs. **3** Le validateur approuve l'autorisation. **6** Le validateur valide l'opération.	**2** Le système affiche l'interface de gestion des autorisation utilisateurs. **4**Le système affiche l'interface de confirmation. **5** Le système exécute l'opération, affiche un message de validation et enregistre l'opération de suppression dans le fichier log. **7** Le système envoie un email à l'administrateur.
Scenario d'erreur	
E1 : Autorisation existe - Le système affiche un message d'erreur - Le scenario ajouter autorisation utilisateur ou groupe reprend au point **2.**	

11.2- Diagramme de séquence du cas d'utilisation<< Gestion des Autorisation>>


Administrateur
Application WEB
Systeme de gestion de Base des données
Ref
Authentification WEB
Ajouter une Autorisation utilisateur
Demande de l'interface gestion autorisation utilisateur
Affiche l'interface gestion autorisation utilisateur
Sélectionne l'utilisateur + la ressource et valide l'opération
Requéte1() Sauvgarde de l'autorisation
Exécution
Resultats de la requéte
Alt
Autorisation n'existe pas
Affiche un message de validation de l'ajout
Ecriture de l'opération dans le fichier log
Autorisation existe
Affiche un message d'erreur
Supprimer autorisation utilisateur
Demande de l'interface gestion autorisation utilisateur
Affiche l'interface gestion autorisation utilisateur
Sélectionne l'autorisation a supprimer
Affiche l'interface de confirmation
Confirme l'opération
Requéte2() Suppression
Exécution
Resultats de la requéte
Ecriture de l'opération dans le fichier log
Affiche un message de validation

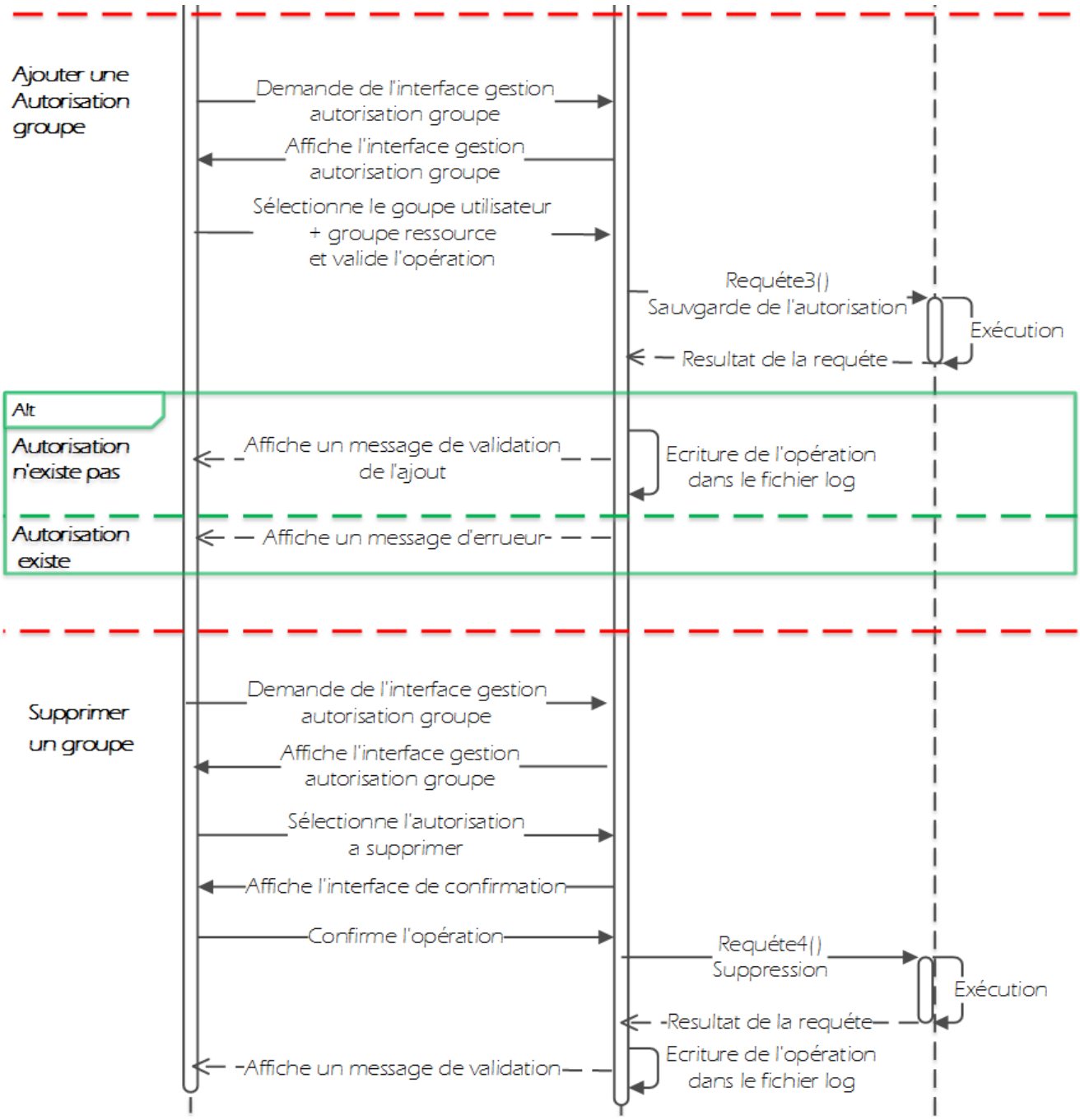


Figure 24 : Diagramme de séquence du cas d'utilisation << Gestion des autorisations>>

11.3- Diagramme de séquence du cas d'utilisation <<Valider les autorisations>>

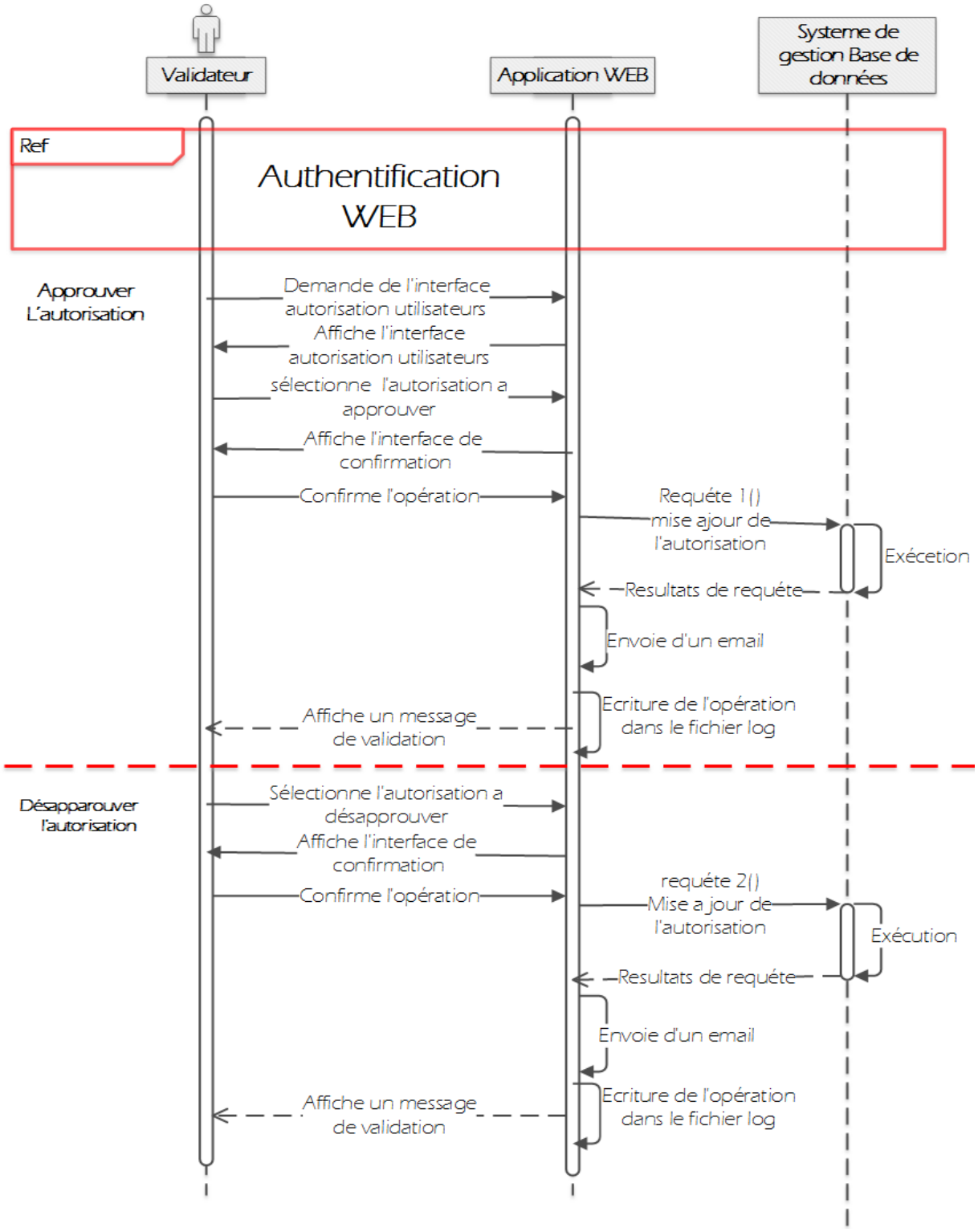


Figure 25 : Diagramme de séquence du cas d'utilisation<<Valider les autorisations>>

12- Cas d'utilisation << Gestion des Commandes interdites >>

La gestion des commandes interdites est l'une des tâches de l'administrateur, elle se compose de 3 sous parties :

i. La gestion des commandes : l'administrateur peut ajouter, supprimer ou importer un fichier de commandes.
ii. La gestion des listes de commande interdite : l'administrateur peut créer des listes de commande interdite à l'exécution et affecte des commandes a cette liste.
iii. La gestion des permissions : l'administrateur peut affecter aux utilisateur une liste de commande interdite, celle-ci interdit aux utilisateurs l'exécution des commandes de cette liste sur leur ressource autorisée, en plus l'administrateur peut supprimer ces affectations.

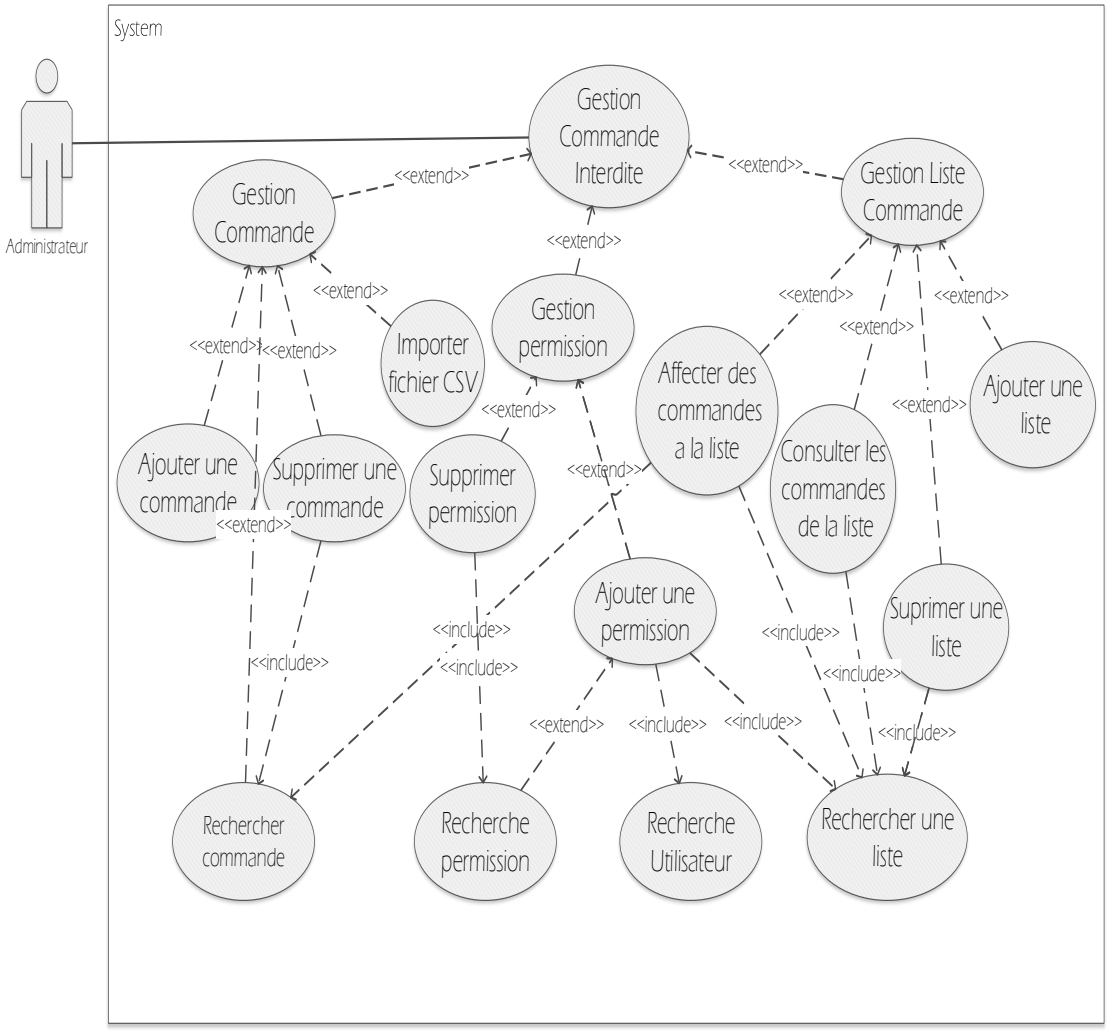


Figure 26 : Diagramme de cas d'utilisation << gestion des Commandes interdites>>

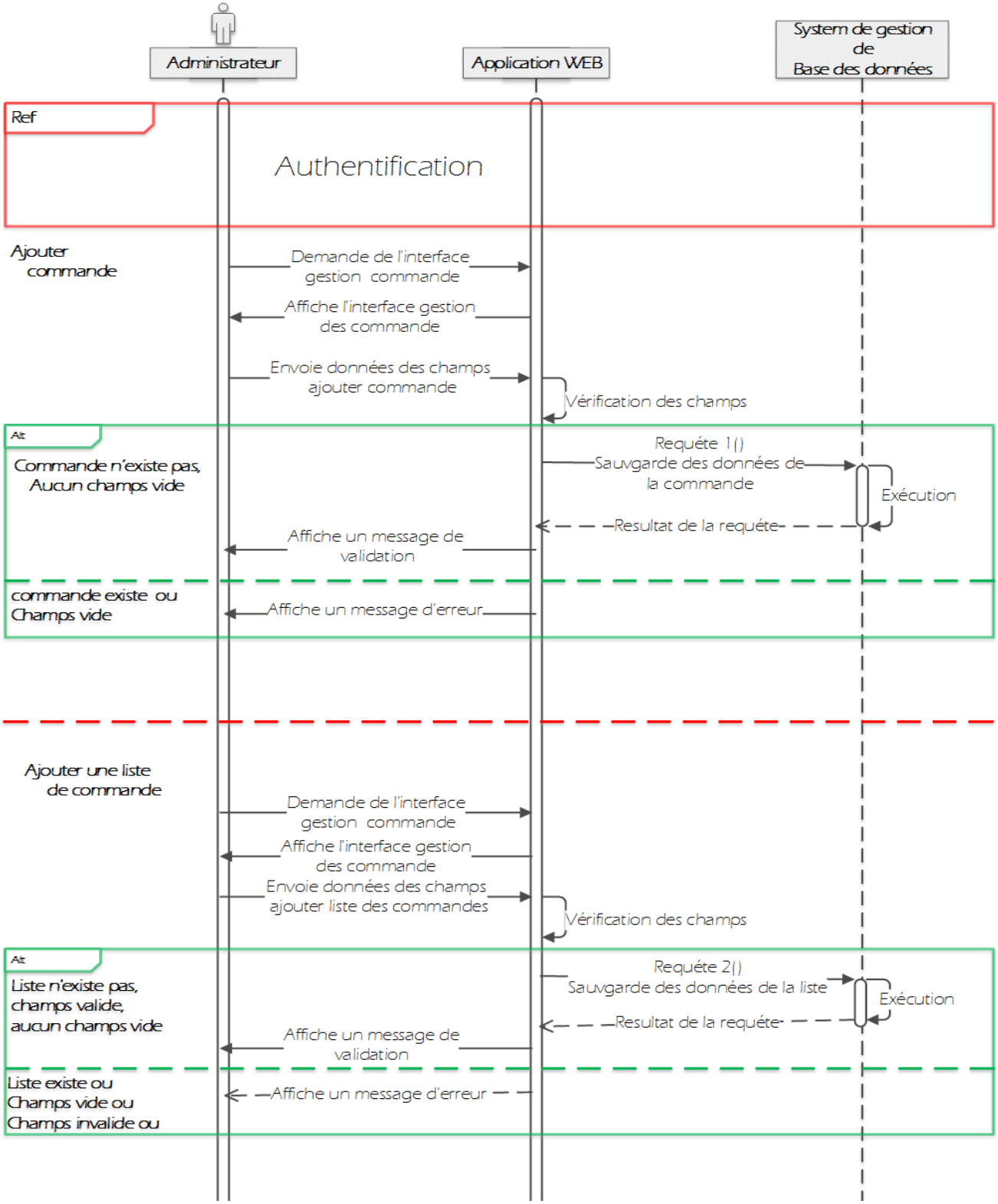
12.1- Description textuelle du cas d'utilisation << Gestion des commandes interdites >>

Sommaire d'identification	
Titre	Gestion des commandes interdites
But	Définir des listes des commandes interdites et les affecter aux utilisateurs
Résume	L'administrateur peut créer et gérer les commandes interdites et l'affectation aux utilisateurs en utilisent les opérations ajout, recherche, affectation et suppression.

Acteur	Administrateur
Description des enchainements	
Préconditions	Post conditions
- Administrateur et authentifié. - L'administrateur à demander l'interface gestion des commandes interdite.	- la gestion des commandes interdite
Scenario : Ajouter commande	
User	Système
1 L'administrateur demande l'interface gestion des commandes. **3** L'administrateur remplit le champ d'ajout commande est valide l'opération.	**2** Le système affiche l'interface gestion des commandes. **4** Le système vérifie les champs et affiche le résultat.
Scenario : Ajouter une liste	
1 L'administrateur remplit le champ d'ajout liste des commandes est valide l'opération. **3** L'administrateur remplit les champs du formulaire est valide l'opération.	**2** Le système vérifie les champs et affiche le résultat. **4** Le système vérifie les champs et affiche le résultat.
Scenario : Affecter des commandes	
1 L'administrateur choisie l'opération affecter une commande a la liste. **3** L'administrateur sélectionne les commandes à affecter et valide l'opération.	**2** Le système affiche la liste des commandes. **4** le système exécute l'opération et affiche un message de validation.

Scenario : Ajouter une permission	
1 L'administrateur demande l'interface gestion permission. **3** L'administrateur sélectionne l'utilisateur et la liste de commande et valide l'opération.	**2** Le système affiche l'interface gestion des permissions. **4** le système exécute l'opération, affiche un message de validation et enregistre l'opération dans un fichier log.
Scenario d'erreur	
E1 : champs vides - le système renvoi un message d'erreur - le scenario ajouter commande reprend au point 2 - le scenario ajouter liste des commandes reprend au point 1 E2 : caractère non autorisé - le système renvoi un message d'erreur - le scenario ajouter commande reprend au point 2 - le scenario ajouter liste des commandes reprend au point 1 E3 : commande existe - le système renvoi un message d'erreur - le scenario ajouter commande reprend au point 2 E4 : liste existe - le système renvoi un message d'erreur - le scenario ajouter liste des commandes reprend au point 1 E5 : permission existe - le système renvoi un message d'erreur - le scenario ajouter permission reprend au point 2	

12.2- Diagramme de séquence du cas d'utilisation<<gestion des commandes interdite>>



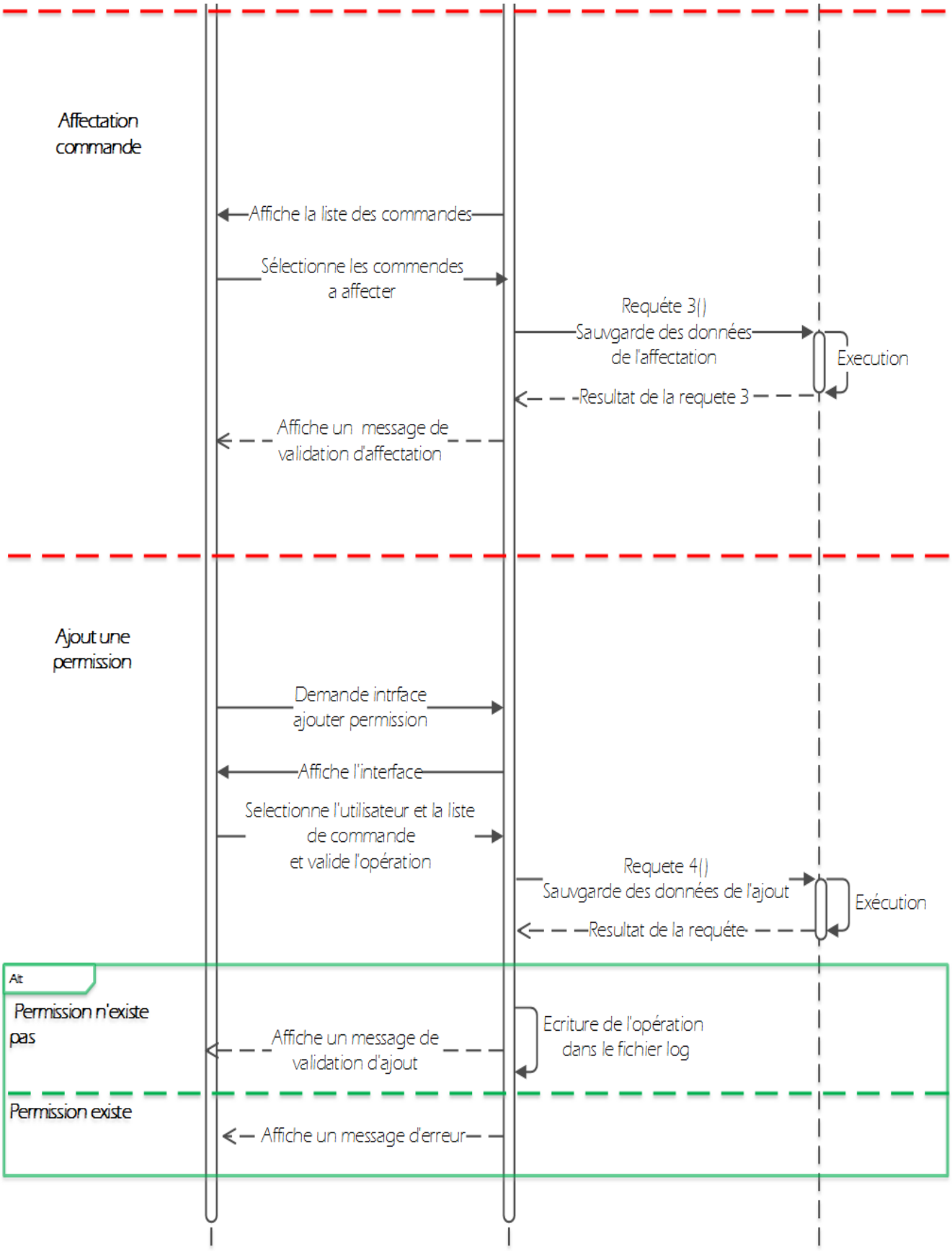

Affectation commande
Affiche la liste des commandes
Sélectionne les commendes a affecter
Requéte 3()
Sauvgarde des données de l'affectation
Execution
Resultat de la requete 3
Affiche un message de validation d'affectation
Ajout une permission
Demande intrface ajouter permission
Affiche l'interface
Selectionne l'utilisateur et la liste de commande et valide l'opération
Requete 4()
Sauvgarde des données de l'ajout
Exécution
Resultat de la requéte
Alt
Permission n'existe pas
Affiche un message de validation d'ajout
Ecriture de l'opération dans le fichier log
Permission existe
Affiche un message d'erreur

Figure 27 : Diagramme de séquence du cas d'utilisation << Gestion des commandes interdite >>

13- Cas d'utilisation <<Consultation des logs>>

L'auditeur peut consulter les logs des session SSH et Web des utilisateurs.

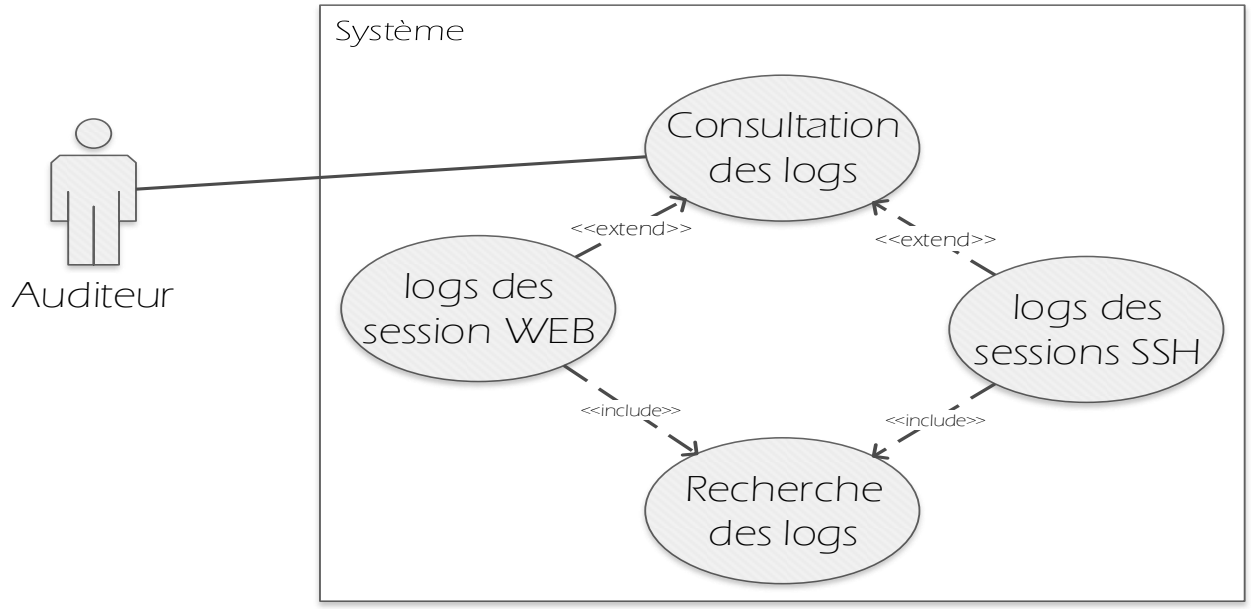


Figure 28 : Diagramme de cas d'utilisation consultation des logs

13.1- Description textuelle du cas d'utilisation << consultation des logs>>

Sommaire d'identification	
Titre	Consultations des logs
But	- Historique des connexions. - Traçabilité des utilisateurs
Résume	L'auditeur peut consulter les fichier logs des session WEB. L'auditeur peut consulter les fichiers logs des session SSH.
Acteur	Auditeur
Description des enchainements	

Préconditions	Post conditions
- Auditeur est authentifier.	- Consultation des logs.

Scenario nominale	
User	Système
1 L'auditeur demande la liste des logs. **3** L'auditer sélectionne le fichier log. **5** L'auditeur consulte le fichier log.	**2** Le système affiche la liste des logs. **4** le système affiche le fichier log.

13.2- Diagramme de séquence du cas d'utilisation<<Consultation des logs>>

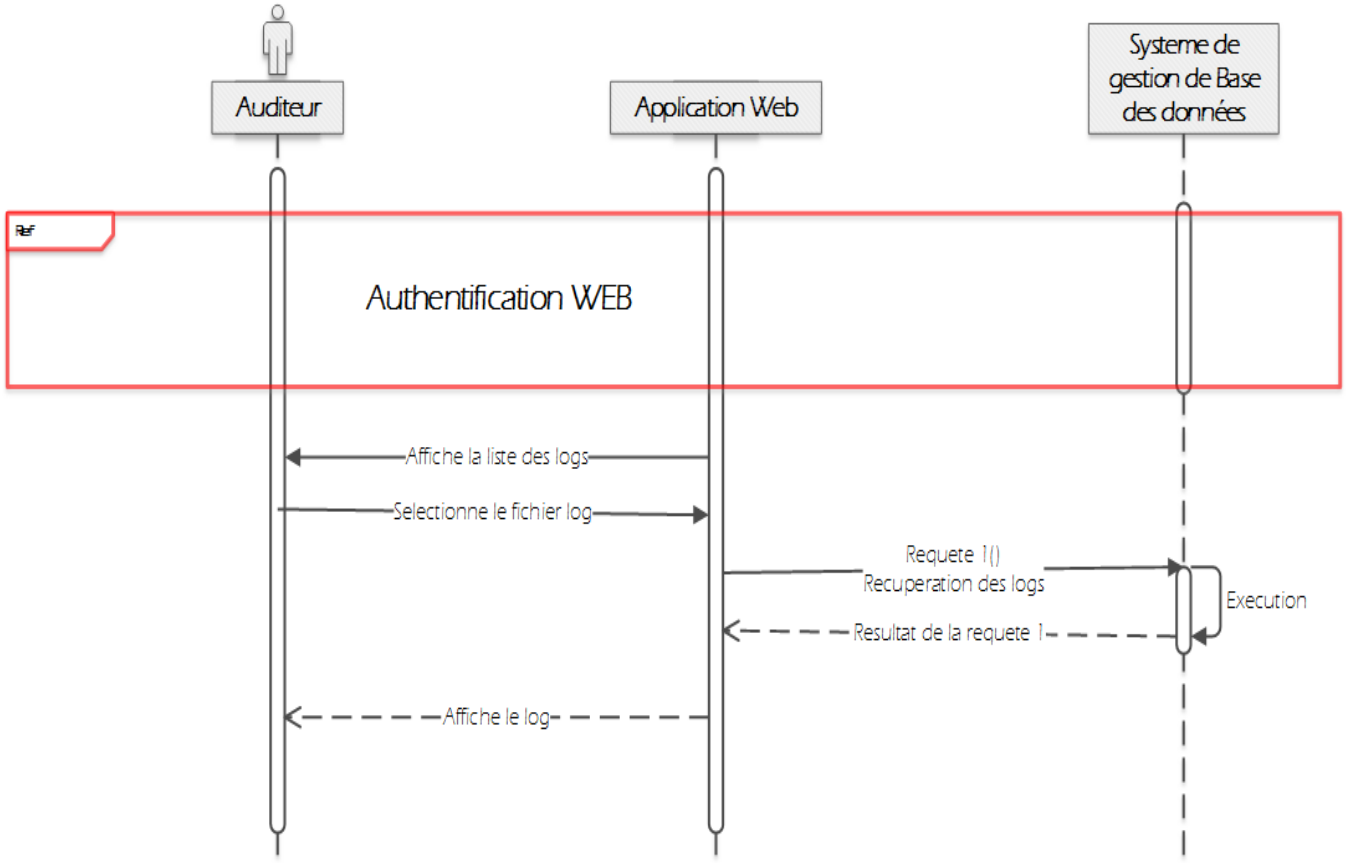


Figure 29 : Diagramme de séquence du cas d'utilisation << Consultation des logs >>

14- Diagramme de classe

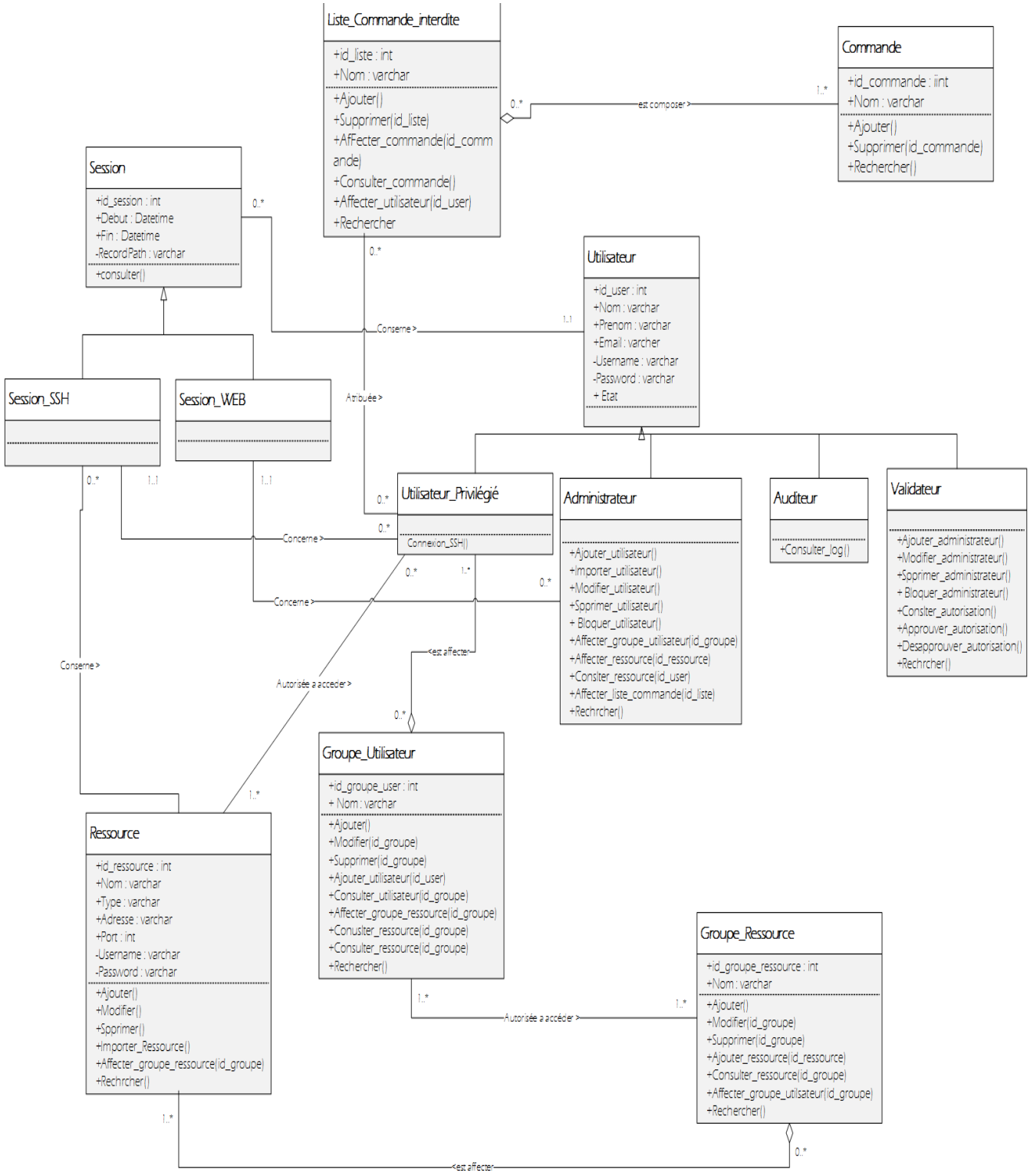


Figure 30 : Diagramme de classe.

15- Schéma relationnel de la base des données :

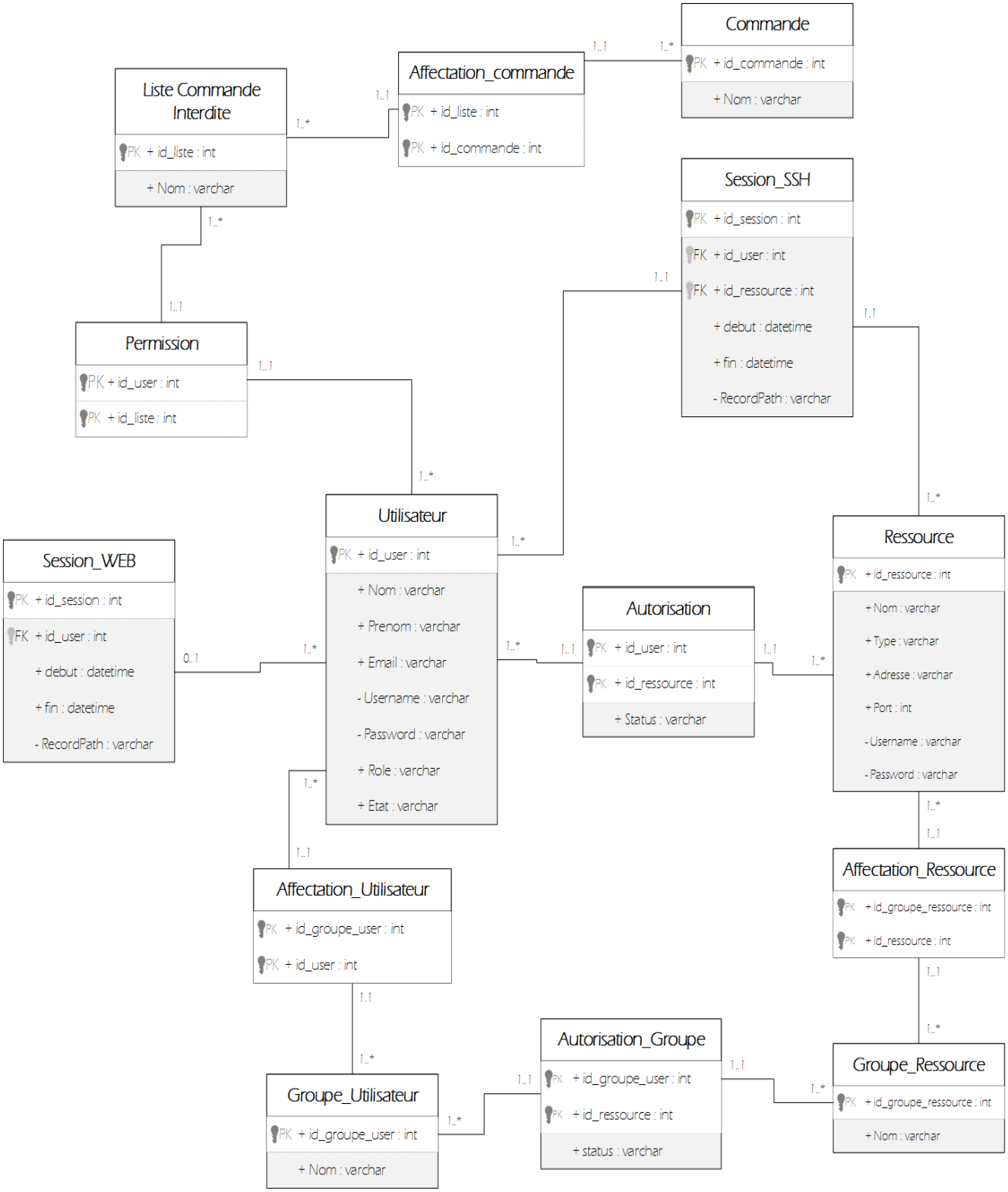


Figure 31 : Schéma relationnel de la base des données

16- Dictionnaire des données

Table	Attributs	Type	Désignation	index
Utilisateur	Id_user	Int	Identifient de l'utilisateur	Clé primaire
	Nom	Varchar	Nom de l'utilisateur	
	Prenom	Varchar	Prénom de l'utilisateur	
	Email	Varchar	Email de L'utilisateur	unique
	Username	Varchar	Attribut qui va être utiliser pour l'authentificatio n	unique
	Password	Varchar	Attribut qui va être utiliser pour l'authentificatio n	
	Etat	varchar	Attribut qui représente l'etat de l'utilisateur (Actif, Bloquer, supprimer).	
	Role	Varchar	Rôle de l'utilisateur (Administrateur, Utilisateur,	

			validateur, Auditeur)	
Ressource	id_ressource	Int	Identifiant de la ressource	Clé primaire
	Nom	Varchar	Nom de la ressource	unique
	Type	Varchar	Type de la ressource (Serveur, router …)	
	Adresse	Varchar	Adresse IP de la ressource	unique
	Port	Int	Le port utiliser pour se connecter à la ressource	
	Username	Varchar	Attribut qui va être utiliser pour l'authentification de l'utilisateur sur la ressource	unique
	Password	Varchar	Attribut qui va être utiliser pour l'authentification de l'utilisateur sur la ressource	
	Id_Session	Int	Identifient de la session	Clé primaire

	Id_user	Int	Identifient de l'utilisateur	Clé étrangère
	Id_ressource	Int	Identifient de la ressource	Clé étrangère
	Debut	Datetime	Date et heure du début de la session	
	Fin	Datetime	Date et heure de la fin de la session	
	Record_Path	varchar	L'emplacement du fichier log	
Session WEB	Id_Session	Int	Identifient de la session	Clé primaire
	Id_User	Int	Identifient de l'utilisateur	Clé étrangère
	Debut	Datetime	Date et heure du début de la session	
	Fin	Datetime	Date et heure de la fin de la session	
	Record_Path	varchar	L'emplacement du fichier log	
Groupe_Utilisateur	Id_groupe_utilisateur	Int	Identifient du groupe utilisateur	Clé primaire
	Nom	varchar	Nom du groupe	unique

Groupe_Ressource	Id_groupe_ressource	Int	Identifient du groupe ressource	Clé primaire
	Nom	varchar	Nom du groupe	unique
Autorisation_Groupe				
	Id_groupe_utilisateur	Int	Identifient du groupe utilisateur	Clé primaire
	Id_groupe_ressource	Int	Identifient du groupe ressource	Clé primaire
	Status	Varchar	Attribu qui représente l'approuvation de l'autorisation	
Autorisation				
	Id_user	Int	Identifient de l'utilisateur	Clé primaire
	Id_ressource	Int	Identifient de la ressource	Clé primaire
Affectation_Utilisateur				
	Id_groupe_user	Int	Identifient du groupe utilisateur	Clé primaire
	Id_user	Int	Identifient de l'utilisateur	Clé primaire

Affectation_Ressource	Id_groupe_ressource	Int	Identifient du groupe ressource	Clé primaire
	Id-ressource	Int	Identifient de la ressource	Clé primaire
Permission				
	Id_user	Int	Identifient de l'utilisateur	Clé primaire
	Id_liste	Int	Identifient de la liste des commandes interdite	Clé primaire
Liste_Commande	Id_liste	Int	Identifient de la liste des commandes interdite	Clé primaire
	Nom	varchar	Nom la liste	unique
Affectation_Commande				
	Id_liste	Int	Identifient de la liste des commandes interdite	Clé primaire
	Id_commande	Int	Identifient de la commande	Clé primaire
Commande	Id_commande	Int	Identifient de la commande	Clé primaire
	Nom	varchar	Nom de la commande	unique

17- Conclusion

Nous avons présenté dans ce chapitre la phase de conception de notre projet qui contient l'architecture globale, les diagrammes des cas d'utilisation et les diagrammes de séquence, qui nous ont aidés à décrire d'une façon détaillée, le fonctionnement de système dans le but de faciliter la réalisation. Ensuit nous avons conçu le diagramme de classe de notre système qui illustre d'une manière globale la structure des éléments qui constitue la base de données associée à notre application.

Dans le chapitre suivant nous entamons l'étape finale de notre projet qui est l'étape de réalisation et développement.

Chapitre 4 :

Réalisation et Tests

1- Introduction

Ce chapitre constitue le dernier volet de ce mémoire, il traite la phase qui a pour objectif l'implémentation de notre application. Nous commençons, tout d'abord, par la description de l'environnement matériel et logiciel utilisés pour développer notre solution. Ensuite nous justifions nos choix technologiques utilisés. Finalement nous donnons un aperçu sur le travail réalisé.

2- Mise en œuvre de l'application

2.1- Outils matériels

Afin de réaliser notre application nous avons utilisé comme matériels un hôte DELL équipé de :

- Processor Intel i7 (quad core).
- Ram 12 Go.
- Windows 7.

On a déployé sur cet hôte plusieurs machines virtuelles :

- **Serveur principale**: Ce serveur a 2 rôles principaux :
  - Héberger notre application web et la base des données MySQL.
  - Déploiement du proxy SSH.

  Il est équipé de:

  - Processeur Intel i7 (1 core)
  - Ram 4 Go.
  - Système d'exploitation : Ubuntu server 17.10

- **Serveurs secondaires** : on a utilisé 2 serveurs secondaires
  1. **Serveur test :** ce serveur a le rôle d'un serveur de test, équipé de :
     - Processeur Intel i7 (1 core).

- Ram 3Go.
- Système d'exploitation : Ubuntu server 17.10.

2. **Serveur AD** : c'est un serveur active directory, on l'utilise pour récupérer les données des utilisateurs et des ressources, il est équipé de :
   - Processeur Intel i7(1 core)
   - Ram 3 Go.
   - Système d'exploitation : Windows server 2016

2.2- Outils logiciel

2.2.1- Application web

❖ PHP

PHP *(Hypertext Preprocessor)* ,plus connu sous son sigle *PHP* (acronyme récursif), est un langage de programmation libre, principalement utilisé pour produire des pages Web dynamiques via un serveur HTTP, mais pouvant également fonctionner comme n'importe quel langage interprété de façon locale. PHP est un langage impératif orienté objet.

PHP a permis de créer un grand nombre de sites web célébré, comme Facebook, Wikipédia, etc. Il est considéré comme des bases de la création de sites web dites dynamique mais également des applications web. La version actuelle est la version 7.2.8, sortie le 19 juillet 2018. [15]

Figure 32: Logo PHP

➢ Bibliothèque PHP ajouté

1. PHP ldap

PHP ldap est une bibliothèque Permet la connexion et l'envoi de requêtes sur un annuaire LDAP, c'est-à-dire un serveur permettant de stocker des informations de manière hiérarchique. Un serveur LDAP est conçu pour être capable de gérer les opérations suivantes

- Établir la connexion avec l'annuaire.
- Rechercher des entrées.
- Comparer des entrées.
- Ajouter des entrées.
- Modifier des entrées.
- Supprimer des entrées.
- Annuler ou abandonner une opération.
- Fermer la connexion avec l'annuaire.

Ainsi cette bibliothèque fournit un ensemble de fonctions permettant de réaliser ces opérations.

- **Installation**

- **Sous Windows**

1. Ajouter les deux bibliothèques libeay32.dll et ssleay32.dll dans le Repertoire php .
2. Activer l'extension ldap dans le fichier php.ini.
3. Redémarrer le service Apache.

- **Sous Linux**

1. Utiliser la commande 'apt-get install php7.0-ldap' (7.0 est la version de PHP sur la machine).
2. Activer l'extension ldap dans le fichier php.ini.
3. Redémarrer le service Apache

- **Exemple de code source**

```php
<?php

    $ldap_dn = "cn=read-only-admin,dc=example,dc=com";
    $ldap_password = "password";

    $ldap_con = ldap_connect("ldap.forumsys.com");

    ldap_set_option($ldap_con, LDAP_OPT_PROTOCOL_VERSION, 3);

    if(ldap_bind($ldap_con, $ldap_dn, $ldap_password)) {

      echo "connexion établie";

    } else {


      echo "Echec de connexion!";
    }
?>
```

Figure 33 : Exemple PHP_Ldap.

2- PHP mailer

PHP mailer est une bibliothèque logicielle d'envoi d'e-mails en PHP. En effet, envoyer un email en code natif exige un haut niveau de connaissance des normes SMTP, du format des emails (tels que l'HTML et le retour chariot), et des vulnérabilités d'injection pour spammer.

Depuis 2001, PHP Mailer est l'une des solutions email les plus populaires en PHP. [16]

- **Installation**

L'installation de PHP Mailer est assez simple. Il faut dézipper le fichier dans le répertoire racine de votre serveur Web référencé par la variable DocumentRoot dans le fichier de configuration d'Apache (httpd.conf) Sur Linux, même procédure que pour Windows.

Lorsque les fichiers ont été décompressés, vous pouvez les inclure dans vos scripts PHP via la fonction include.

- **Méthode d'envoi**

Avec PHP Mailer, il y a deux méthodes pour envoyer des e-mails.

- La méthode SMTP permettant de se connecter à un serveur de mail distant
- La méthode "mail" lorsque le serveur de mail est local

La méthode SMTP peut également être utilisée avec un serveur local mais il est préférable de privilégier la méthode "mail" avec un serveur local car elle est plus rapide.

❖ Bootstrap

Bootstrap est une collection d'outils utiles à la création du design (graphisme, animation et interactions avec la page dans le navigateur ... etc. ...) de sites et d'applications web. C'est un ensemble qui contient des codes HTML et CSS, des formulaires, boutons, outils de navigation et autres éléments interactifs, ainsi que des extensions JavaScript en option. C'est l'un des projets les plus populaires sur la plate-forme de gestion de développement GitHub.

Figure 34 : Logo bootstrap

❖ Apache server

Apache Web Server est un logiciel de création, de déploiement et de gestion de serveur Web open source. Initialement développé par un groupe de programmeurs, il est désormais géré par *Apache Software Foundation*.

Apache Web Server est conçu pour créer des serveurs Web pouvant héberger un ou plusieurs sites Web HTTP. Les fonctionnalités remarquables incluent la possibilité de prendre en charge plusieurs langages de programmation, les scripts côté serveur, un mécanisme d'authentification

et la prise en charge de bases de données. Apache Web Server peut être amélioré en manipulant la base de code ou en ajoutant plusieurs extensions / add-ons.

Il est également largement utilisé par les sociétés d'hébergement Web pour fournir un hébergement partagé / virtuel, car, par défaut, Apache Web Server prend en charge et distingue les différents hôtes résidant sur le même ordinateur.

Figure 35 : Logo Apache

2.2.2- Serveur proxy « SSH »

❖ **Python**

Python est un langage de script de haut niveau, structuré et open source. Il est multi-paradigme et multi-usage. Développé à l'origine par Guido van Rossum en 1989, il est, comme la plupart des applications et outils open source, maintenu par une équipe de développeurs un peu partout dans le monde.

Conçu pour être orienté objet, il n'en dispose pas moins d'outils permettant de se livrer à la programmation fonctionnelle ou impérative ; c'est d'ailleurs une des raisons qui lui vaut son appellation de « langage agile ».

Parmi les autres raisons, citons la rapidité de développement (qualité propre aux langages interprétés), la grande quantité de modules fournis dans la distribution de base ainsi que le nombre d'interfaces disponibles avec des bibliothèques écrites en C, C++ ou Fortran. Il est également apprécié pour la clarté de sa syntaxe.

Figure 36 : Logo Python

➢ Bibliothèque python utilisées

1- Paramiko

"Paramiko" est une combinaison des mots espéranto pour "paranoïaque" et "ami". C'est un module pour Python 2.7 / 3.4 + qui implémente le protocole SSH2 pour des connexions sécurisées (chiffrées et authentifiées) aux machines distantes. Contrairement à SSL, le protocole SSH2 ne nécessite pas de certificats hiérarchiques signés par une autorité centrale puissante. Vous connaissez peut-être SSH2 comme protocole remplaçant Telnet et rsh pour un accès sécurisé aux Shell distants, mais le protocole permet également d'ouvrir des canaux arbitraires vers des services distants via le tunnel crypté (c'est ainsi que fonctionne le SFTP, par exemple).

Il est écrit entièrement en Python (bien qu'il dépende des *wrappers* C tiers pour la cryptographie de bas niveau; ceux-ci sont souvent précompilés) et est publié sous la licence GNU *Lesser General Public License* (LGPL).

- **Installation**

Exécuter '`pip install paramiko`' dans un invité de commande Sous Windows ou Linux.

- **Exemple de code source**

```python
from paramiko import client
class ssh:                  #créez une nouvelle classe
    client = None

    def __init__(self, address, username, password):      #fonction d'initialisation
        print("Connecting to server.")                    #Faites savoir à l'utilisateur que nous nous connectons au serveur
        self.client = client.SSHClient()                  # Créer un nouveau client SSH
        self.client.set_missing_host_key_policy(client.AutoAddPolicy()) """ La ligne suivante est requise si vous souhaitez
                                                                            que le script  puisse accéder à un serveur qui ne
                                                                            figure pas encore dans le fichier known_hosts."""
        self.client.connect(address, username=username, password=password, look_for_keys=False) # Demarrer la connexion

    def sendCommand(self, command):                                  #fonction envoyer des commandes
        if(self.client):                                             # Vérifiez si la connexion est établie précédemment
            stdin, stdout, stderr = self.client.exec_command(command)
            while not stdout.channel.exit_status_ready():
                if stdout.channel.recv_ready():                      # Imprimer les données stdout lorsqu'elles sont disponibles
                    alldata = stdout.channel.recv(1024)              # Récupérer les 1024 premiers octets
                    prevdata = b"1"
                    while prevdata:
                        prevdata = stdout.channel.recv(1024)         # Récupérer les 1024 octets suivants
                        alldata += prevdata
                    print(str(alldata, "utf8"))
        else:
            print("Connection not opened.")                          # Afficher sous forme de chaîne avec l'encodage utf8
```

Figure 37: Exemple PARAMIKO

2- Socket

Python fournit deux niveaux d'accès aux services réseau. À un faible niveau, vous pouvez accéder au support de socket de base dans le système d'exploitation, ce qui vous permet d'implémenter des clients et des serveurs pour les protocoles orientés connexion et sans connexion.

Python possède également des bibliothèques qui fournissent un accès de haut niveau à des protocoles réseau spécifiques au niveau de l'application, tels que FTP, HTTP, etc.

Les sockets sont les extrémités d'un canal de communication bidirectionnel. Les sockets peuvent communiquer dans un processus, entre des processus sur la même machine ou entre des processus sur différents Machines.

Les sockets peuvent être implémentés sur différents types de canaux: sockets de domaine Unix, TCP, UDP, etc. La bibliothèque de *sockets* fournit des classes spécifiques pour gérer les transports communs ainsi qu'une interface générique pour gérer le reste.

- **Exemple de code source**

Un simple serveur :

```
1   !/usr/bin/python            # Il s'agit de fichier Server.py
2   import socket               # Importer le module socke
3
4   s = socket.socket()         # Créer un objet socket
5   host = socket.gethostname() # Récupère le nom de la machine locale
6   port = 12345                # Réservez un port pour votre service.
7   s.bind((host, port))        # Lier au port
8   s.listen(5)                 # Maintenant, attendez la connexion client.
9   while True:
10      c, addr = s.accept()    # Établissez la connexion avec le client.
11      print (Got connection  addr)
12      c.send('Thank you for connecting')
13      c.close()               # Fermer la connexion
```

Figure 38: Un Simple serveur en utilisant socket

Un simple client :

```
1  #!/usr/bin/python          # Ceci est le fichier client.py
2  import socket              # Importer le module socket
3  s = socket.socket()        # Créer un objet socket
4  host = socket.gethostname() # Récupère le nom de la machine locale
5  port = 12345               # Réservez un port pour votre service.s.connect((host, port))
6  print s.recv(1024)
7  s.close                    # Fermez le socket lorsque vous avez terminé
```

Figure 39 : Un Simple client en Utilisent Socket

❖ Client SSH

➢ XShell

Xshell est un puissant émulateur de terminal prenant en charge SSH1, SSH2, SFTP, TELNET, RLOGIN et SERIAL. Offrant des performances de pointe, Xshell inclut une combinaison de fonctionnalités et d'avantages inexistants chez d'autres clients SSH. Les fonctionnalités que les utilisateurs professionnels trouveront utiles incluent un environnement à onglets, le transfert de port dynamique, le mappage de clé personnalisé, les jeux de surbrillance…etc.

Figure 40: Logo Xshell

2.2.3- Base des données

❖ MySQL Server

MySQL est un système de gestion de bases de données relationnelles (SGBDR). Il est distribué sous une double licence GPL et propriétaire. Il fait partie des logiciels de gestion de base de données les plus utilisés au monde, autant par le grand public (applications web principalement) que par des professionnels, en concurrence avec Oracle, PostgreSQL et Microsoft SQL Server.

MySQL est un serveur de bases de données relationnelles SQL développé dans un souci de performances élevées en lecture, ce qui signifie qu'il est davantage orienté vers le service de données déjà en place que vers celui de mises à jour fréquentes et fortement sécurisées. Il est multithread et multi-utilisateur.

Figure 41: *Logo MySQL*

2.2.4- VMware Workstation

VMware Workstation est un outil de virtualisation de poste de travail créé par la société VMware, il peut être utilisé pour mettre en place un environnement de test pour développer de nouveaux logiciels, ou pour tester l'architecture complexe d'un système d'exploitation avant de l'installer réellement sur une machine physique. Aujourd'hui, VMware Workstation Pro est principalement conçu pour créer et gérer plusieurs machines virtuelles simultanées et peut prendre en charge de grandes machines virtuelles utilisant 16 processeurs virtuels (vCPU) et 64 Go .

Figure 42: *Logo VMware*

3- Réalisation

3.1- Partie WEB :

C'est la partie qui permet l'administration de notre solution. Une fois les utilisateurs sont authentifiés, le system les redirige à leur espace personnel tout dépend de leur rôle.

3.1.1- Interface Administrateur

❖ **Gestion des utilisateurs :**

Dans cette partie l'administrateur aura la possibilité de gérer les utilisateurs de notre system, il peut accéder à cette partie en choisissant dans le menu de navigation utilisateur -> Gestion utilisateur, en effet il aura la possibilité de :

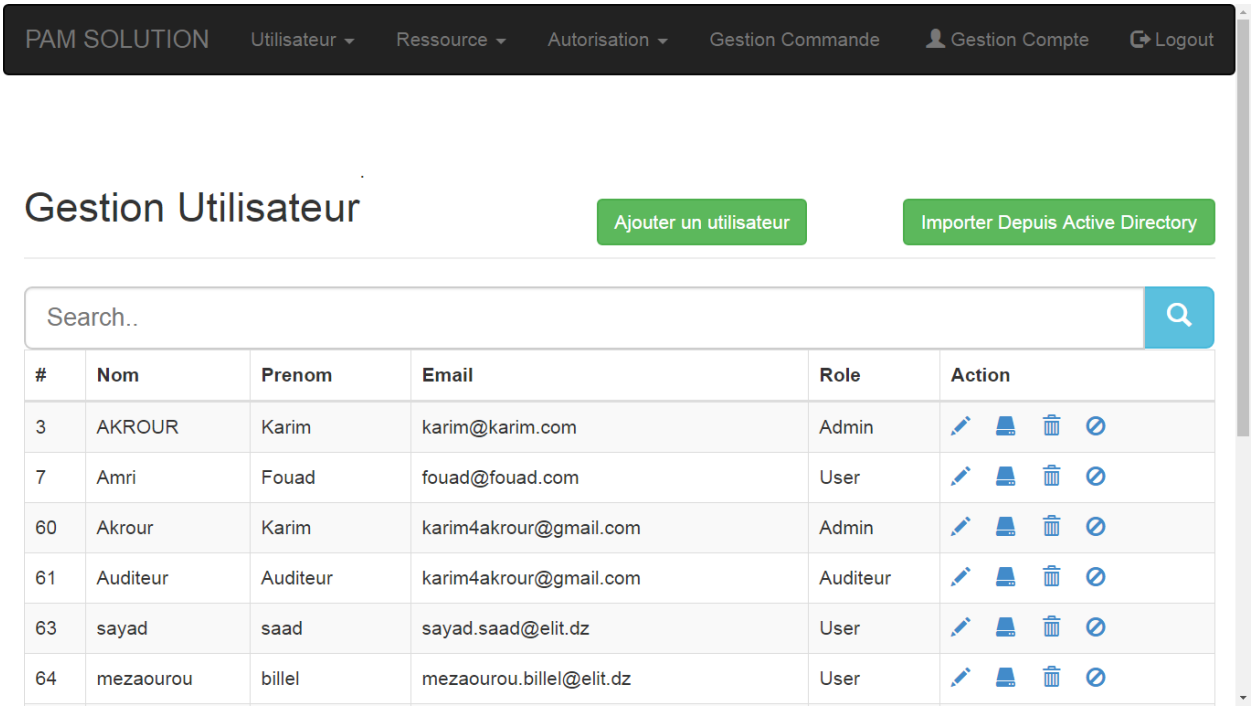


Figure 43: *Interface gestion des utilisateurs.*

- **Ajouter un utilisateur :** lui affiche un formulaire pour remplir les informations de l'utilisateur (Nom, Prénom, Email, Rôle), Un email contenant un « Nom d'utilisateur »

et un « mot de passe » généré aléatoirement sera envoyer à l'adresse Email de l'utilisateur ajouter.

- **Importer utilisateur :** permet à l'administrateur d'importer des utilisateurs directement depuis l'active directory de la société, l'administrateur na que choisir les rôles des utilisateurs à importer, Un email contenant un « Nom d'utilisateur » et un « mot de passe » généré aléatoirement sera envoyer aux utilisateurs importer

Figure 44 : Exemple d'un email envoyer à l'utilisateur

- **Modifier un utilisateur :** l'administrateur peut modifier les informations d'un utilisateur en cliquant sur le bouton un formulaire avec les informations de l'utilisateur sera donc afficher.
- **Consulter les ressources de l'utilisateur :** l'administrateur peut consulter la liste des ressources autorisée d'un utilisateur en cliquant sur le bouton une page contenant la liste de ces ressources sera donc afficher.
- **Supprimer un utilisateur :** l'administrateur peut supprimer un utilisateur en cliquant sur le bouton une page de confirmation sera afficher.
- **Affecté à une liste de commande interdite :** l'administrateur peut affecter un utilisateur a une liste de commande interdite en cliquant sur le bouton une page contenant la liste des commandes interdite sera afficher, l'administrateur choisi les listes à affecter et valide l'opération.

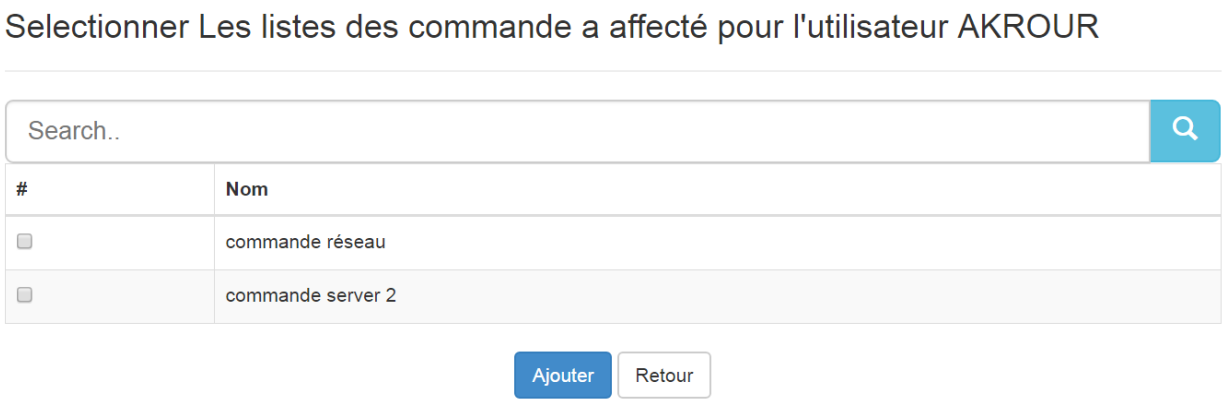


Figure 45 : Interface affectation des listes de commandes à l'utilisateur

❖ **Gestion des groupes utilisateurs** :

Dans cette partie l'administrateur aura la possibilité de géré les groupes d'utilisateurs de notre system, il peut accéder à cette partie en choisissant dans le menu de navigation utilisateur -> Gestion des groupes, il aura la possibilité dans cette partie d'effectuer les opérations suivantes :

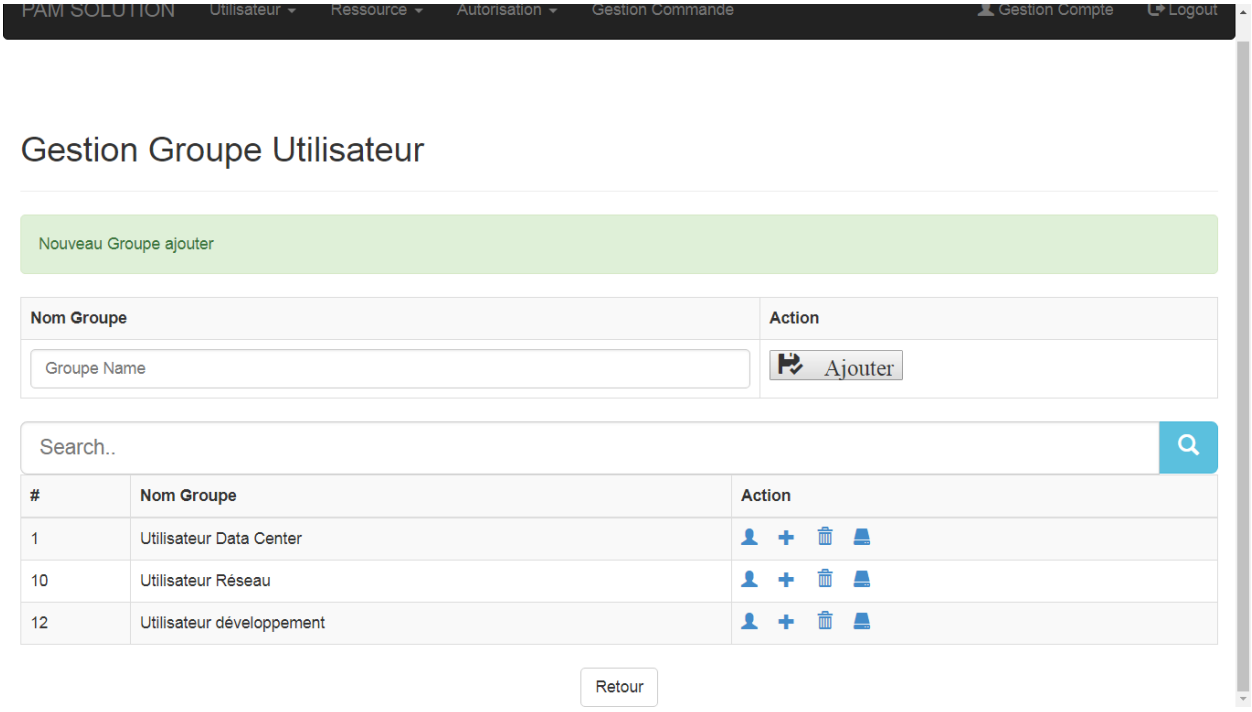


Figure 46 : Interface gestion des groupes utilisateurs.

- **Créer un groupe :** l'administrateur saisie le nom du groupe et clique sur le bouton Ajouter.
- **Gérer un groupe :** l'administrateur aura la possibilité de géré un groupe en cliquant sur le bouton l'interface suivante sera afficher :

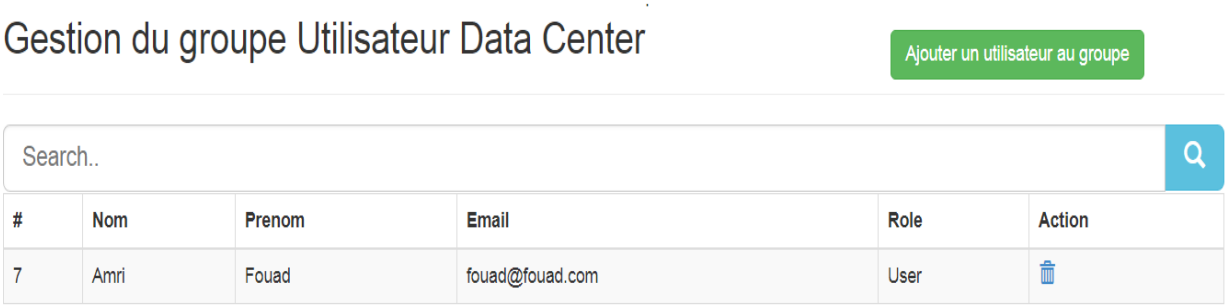


Figure 47 : Interface gestion d'un groupe utilisateur.

Dans cette interface l'administrateur peut :

- Consulter les utilisateurs du groupe.
- Ajouter des utilisateurs au groupe.
- Supprimer des utilisateurs du groupe.

- **Supprimer un groupe :** l'administrateur aura la possibilité de supprimer un groupe en cliquant sur le bouton une page de confirmation sera afficher.
- **Consulter les ressource d'un groupe :** l'administrateur peut consulter la liste des ressources autorisée d'un groupe d'utilisateur en cliquant sur le bouton une page contenant la liste de ces ressources sera donc afficher.

❖ Gestion des ressources

Dans cette partie l'administrateur aura la possibilité de géré les ressources de notre system, il peut accéder à cette partie en choisissant dans le menu de navigation ressource -> Gestion ressource, il aura la possibilité dans cette partie d'effectuer les opérations suivantes:

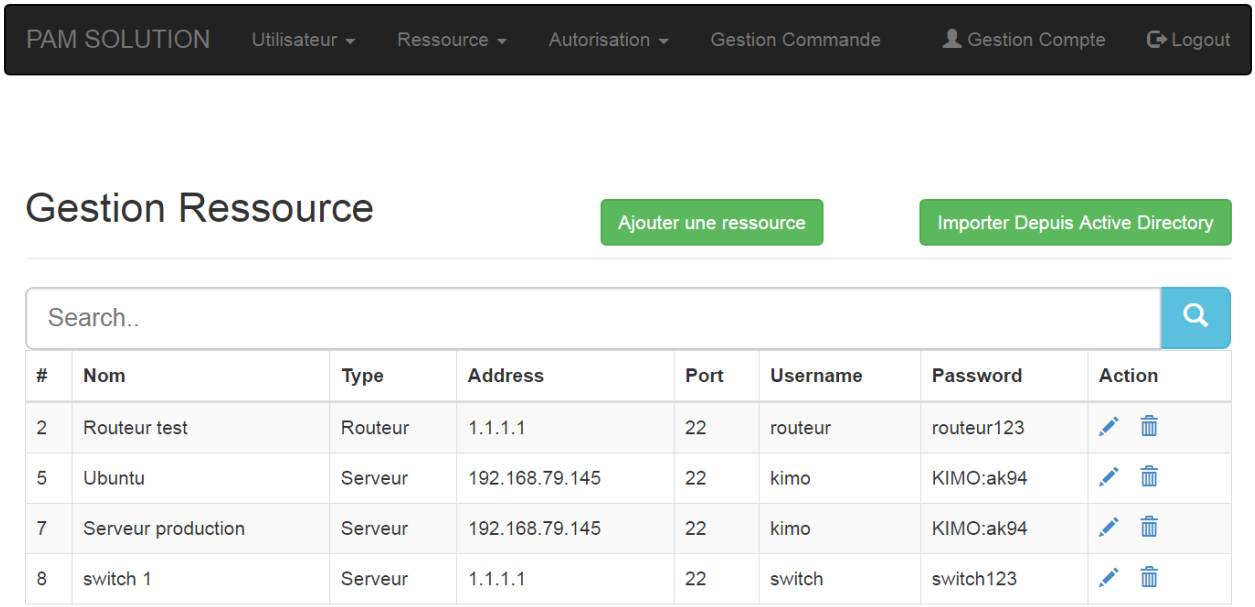


Figure 48 : Interface gestion ressource.

- **Ajouter une ressource :** lui affiche un formulaire pour remplir les informations de la ressource (Nom, Type, Adresse, Port, Username,Password) le Type peut être soit (Routeur ,Serveur, Switch, Pare-feu…..). Après avoir rempli les champs du formulaire l'administrateur clique sur le bouton ajouter pour valider l'opération.

Figure 49 : Formulaire d'ajout d'une ressource.

- **Importer ressource :** permet à l'administrateur d'importer des ressources directement depuis l'active directory de la société, une page contenant les ressources qui sont pas encore ajouter sera afficher, l'administrateur sélectionne les ressources à importer et valide l'opération.
- **Modifier une ressource :** l'administrateur peut modifier les information d'une ressource en cliquant sur le bouton un formulaire avec les informations de la ressource sera donc afficher.
- **Supprimer une ressource :** l'administrateur peut supprimer une ressource en cliquant sur le bouton une page de confirmation sera afficher.

❖ Gestion des groupes ressources

Dans cette partie l'administrateur aura la possibilité de géré les groupes de ressource de notre system, il peut accéder à cette partie en choisissant dans le menu de navigation Ressource -> Gestion des groupes, il aura la possibilité dans cette partie d'effectuer les opérations suivantes :

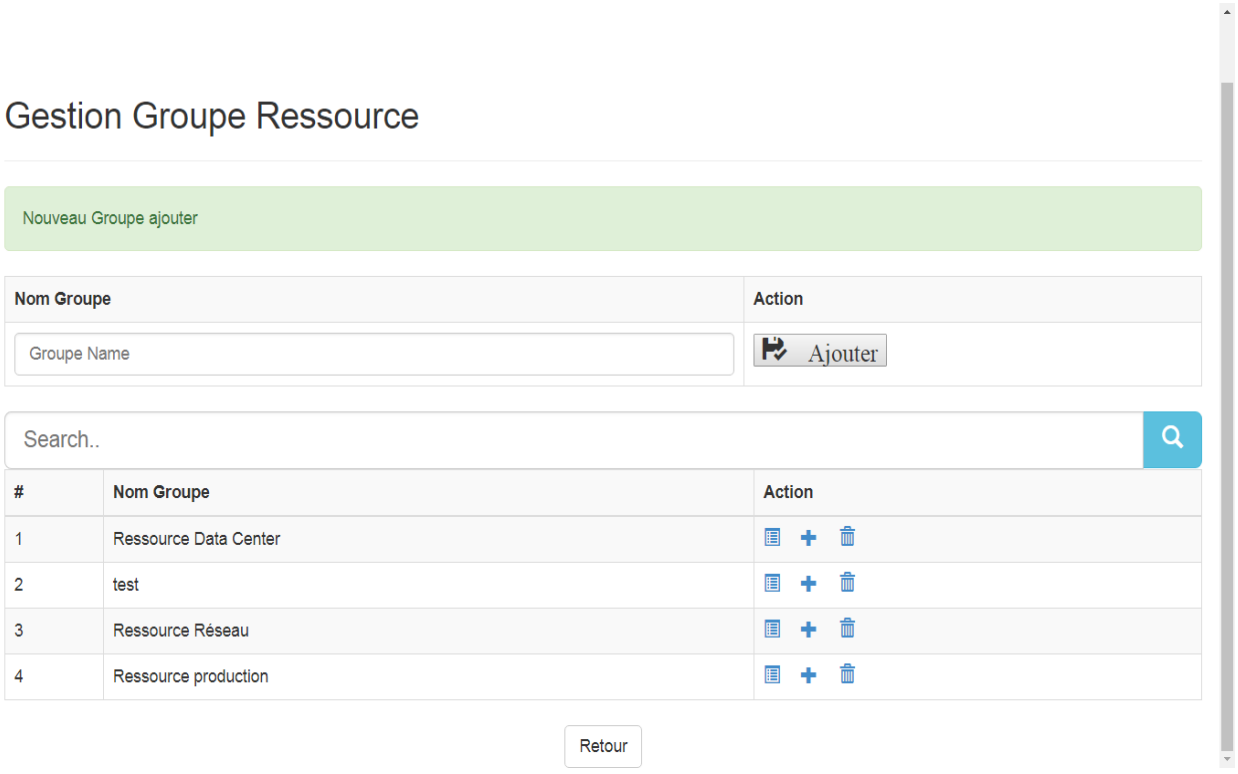


Figure 50 : Interface gestion des groupes ressources.

- **Créer un groupe :** l'administrateur saisie le nom du groupe et clique sur le bouton Ajouter.
- **Gérer un groupe :** l'administrateur aura la possibilité de géré un groupe en cliquant sur le bouton l'interface suivante sera afficher :

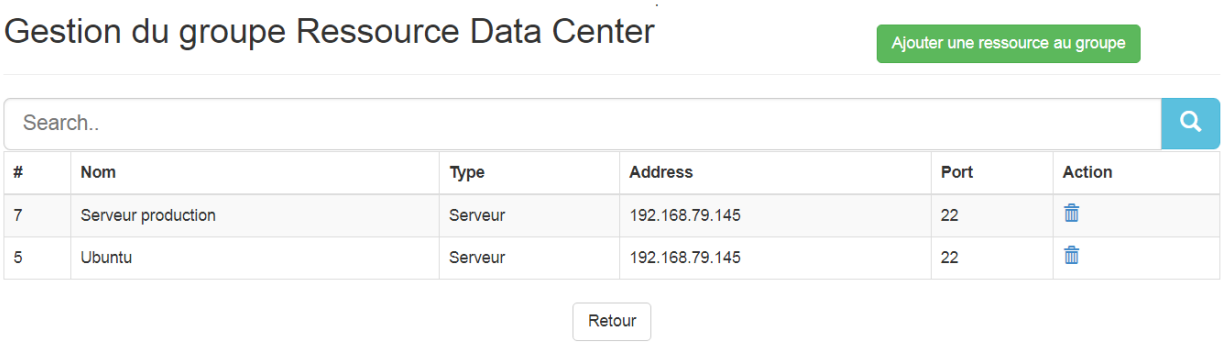


Figure 51 : Interface gestion d'un groupe ressource.

Dans cette interface l'administrateur peut :

- Consulter les ressources du groupe.
- Ajouter des ressources au groupe.
- Supprimer des ressources du groupe.

- **Supprimer un groupe :** l'administrateur aura la possibilité de supprimer un groupe en cliquant sur le bouton une page de confirmation sera afficher.

❖ Gestion des autorisations

Cette Section est diviser en deux partie :

Partie 1 : Gestion autorisation utilisateur

Dans cette partie l'administrateur aura la possibilité de géré les autorisations individuelles pour chaque utilisateur, il peut accéder à cette partie en choisissant dans le menu de navigation Autorisation -> Autorisation utilisateur, il aura la possibilité dans cette partie d'effectuer les opérations suivantes :

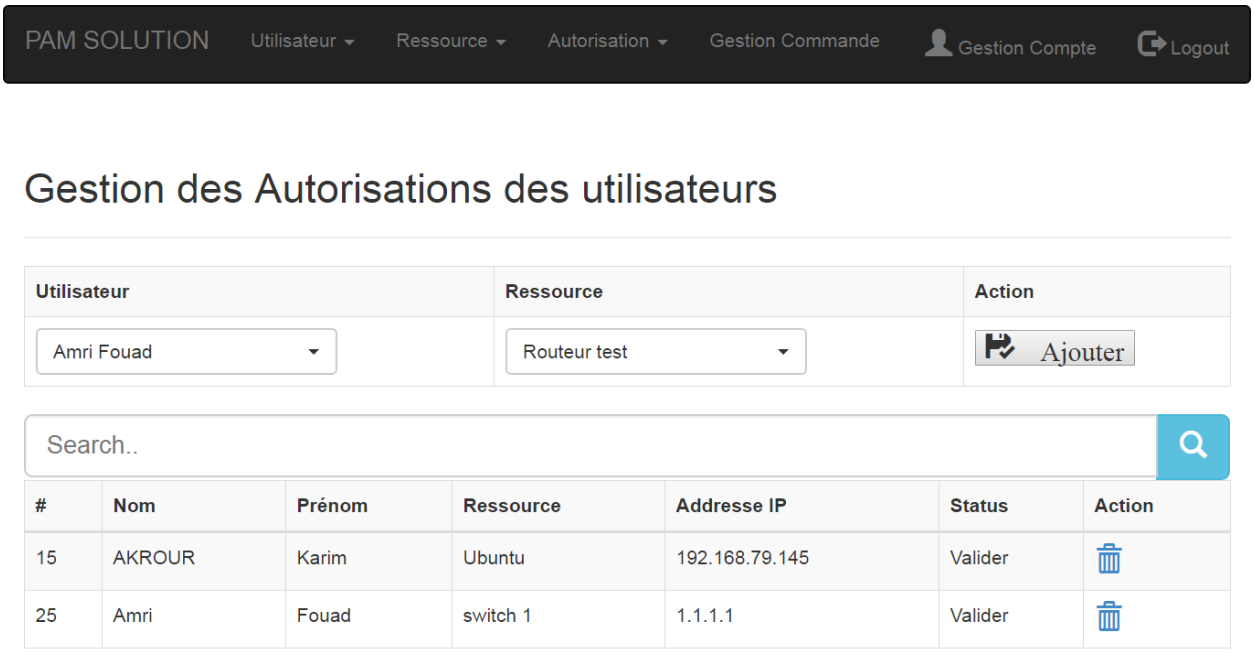


Figure 52: Interface gestion des autorisation des utilisateurs.

- **Ajouter une autorisation :** l'administrateur sélectionne dans les menus déroulante l'utilisateur et la ressource et clique sur le bouton ajouter, l'autorisation sera donc ajoutée avec le statu « En Attente » en attendant que le validateur approuve cette autorisation, l'utilisateur ne peut pas accéder à la ressource qu'après avoir été approuver par le validateur.
- **Supprimer autorisation :** l'administrateur peut supprimer une autorisation en cliquant sur le bouton une page de confirmation sera afficher.

Partie 2 : Gestion autorisation groupe

Dans cette partie l'administrateur aura la possibilité de géré les autorisations des groupes, en effet il aura la possibilité d'affecter directement un groupe d'utilisateur a un groupe de ressource, il peut accéder à cette partie en choisissant dans le menu de navigation Autorisation -> Autorisation groupe, il aura la possibilité dans cette partie d'effectuer les opérations suivantes :

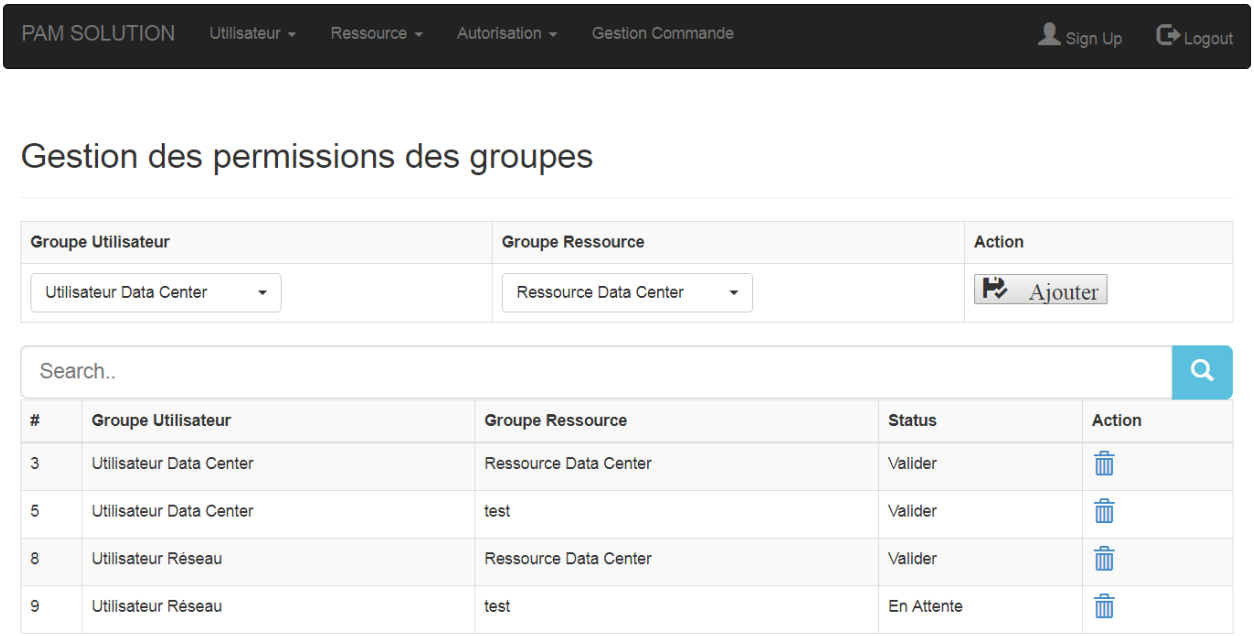


Figure 53 : Interface gestion des autorisations des groupes.

- **Ajouter une autorisation :** l'administrateur sélectionne dans les menus déroulants le groupe d'utilisateur et le groupe de ressource et clique sur le bouton ajouter, l'autorisation sera donc ajoutée avec le statu « En Attente » en attendant que le validateur approuve cette autorisation, les utilisateurs du groupe ne pourront pas accéder aux ressources du groupe qu'après avoir été approuver par le validateur.
- **Supprimer autorisation :** l'administrateur peut supprimer une autorisation en cliquant sur le bouton une page de confirmation sera afficher.

❖ Gestion des commandes interdits

Cette section sera diviser en troie partie :

Partie 1 : Gestion commande

Dans cette partie l'administrateur aura la possibilité de géré les commandes interdites, il peut accéder à cette partie en choisissant dans le menu de navigation Gestion commande -> Gestion commande, il aura la possibilité dans cette partie d'effectuer les opérations suivantes :

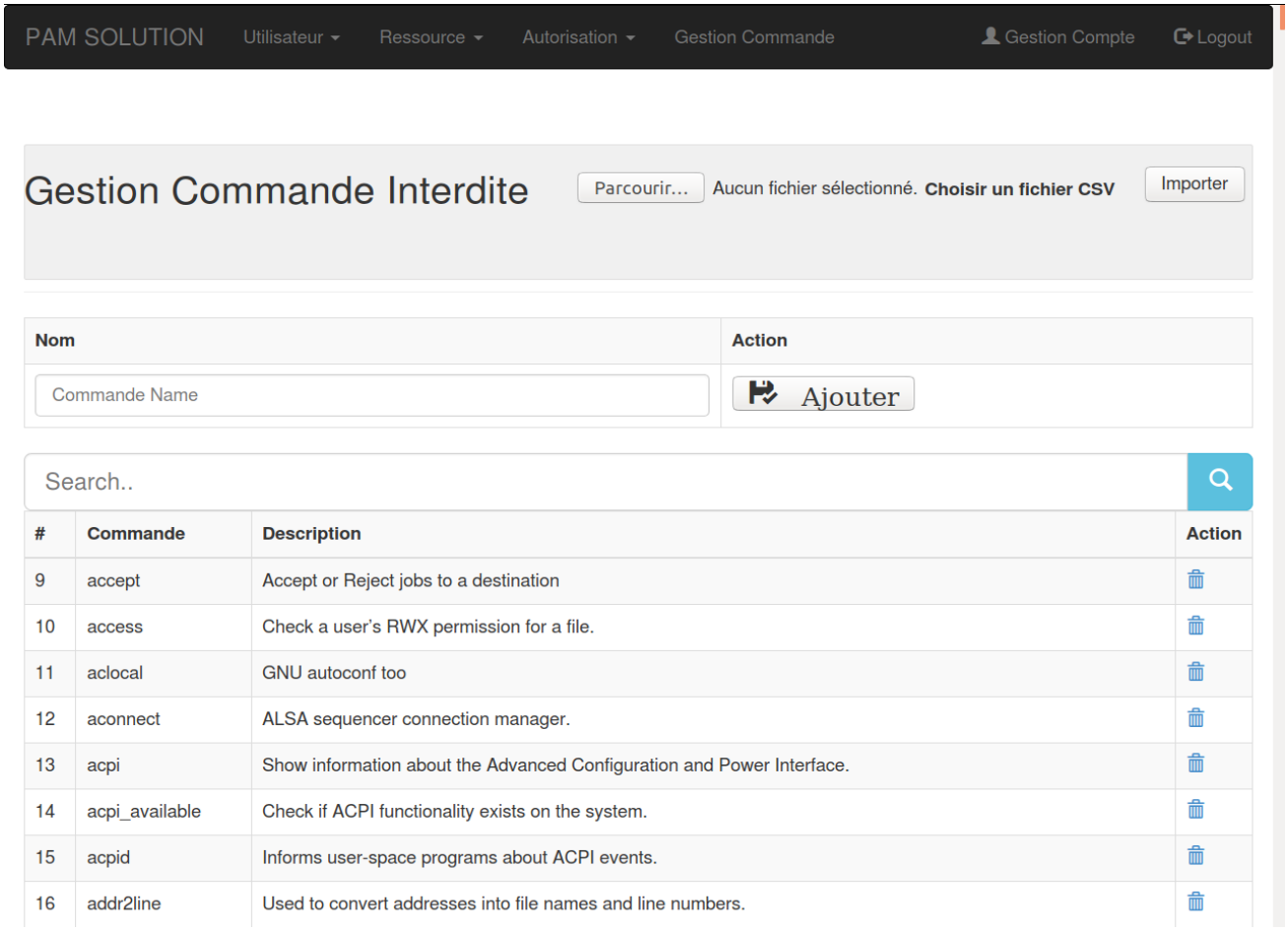


Figure 54 : Interface gestion des commandes interdites

- **Importer un fichier CSV :** pour faciliter la tâche de l'administrateur il aura la possibilité d'importer directement un fichier CSV contenant les commandes system et leur description, pour cela il choisit un fichier et clique sur le bouton
- **Ajouter une commande :** l'administrateur saisie le nom de la commande et sa description et clique sur le bouton ajouter.

- **Supprimer une commande :** l'administrateur peut supprimer une commande en cliquant sur le bouton une page de confirmation sera afficher.

Partie 2 : Gestion liste commande

Dans cette partie l'administrateur peut regrouper les commandes dans des listes pour les affectés ensuite au utilisateur, il peut accéder à cette partie en choisissant dans le menu de navigation Gestion commande, il aura la possibilité dans cette partie d'effectuer les opérations suivantes :

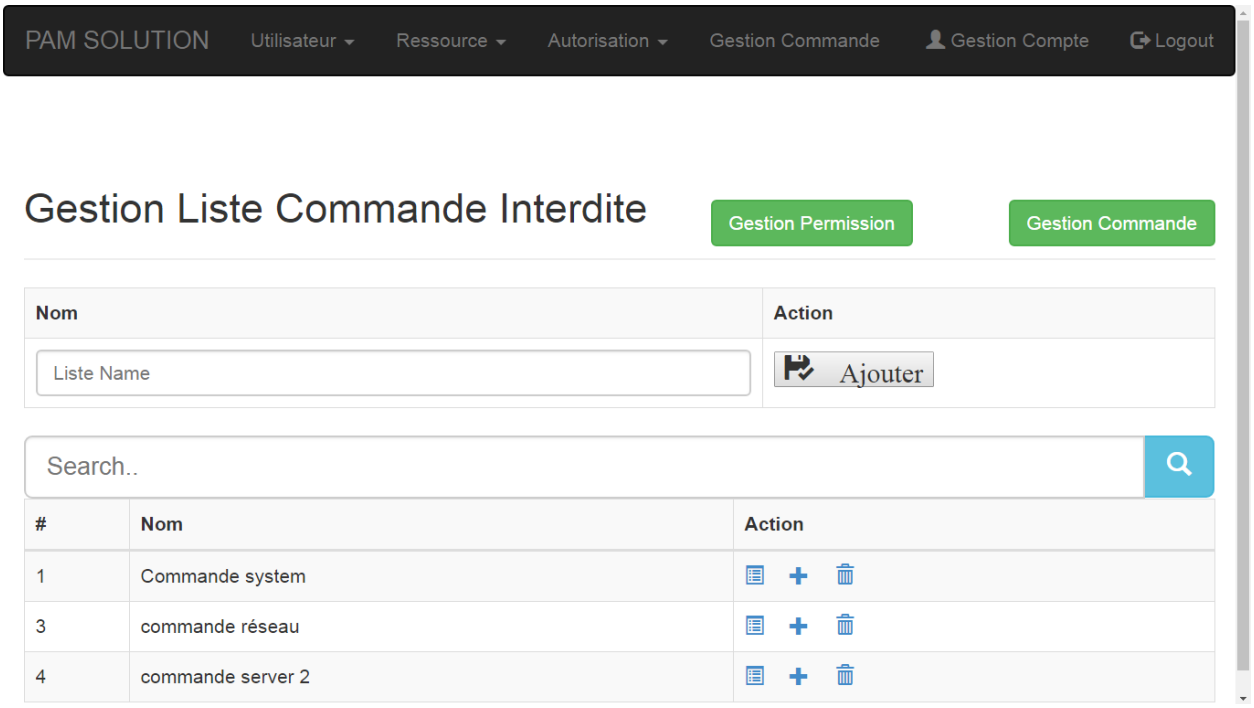


Figure 55 : Interface gestion des listes des commandes interdite.

- **Créer une liste de commande :** l'administrateur saisie le nom de la liste et clique sur le bouton ajouter.
- **Gérer une liste :** l'administrateur peut gérer une liste de commande en cliquant sur le bouton , une nouvelle interface sera afficher lui permettant de :
  - Consulter les commandes de la liste.
  - Ajouter des commandes a la liste.
  - Supprimer des commandes de la liste.

- **Supprimer une liste :** l'administrateur peut supprimer une liste de commande en cliquant sur le bouton une interface de confirmation sera afficher.

Partie 3 : Gestion des permission

Dans cette partie l'administrateur peut affecter des liste de commande interdite aux utilisateur, il peut accéder a cette partie en choisissant dans le menu de navigation Gestion commande -> gestion permission, il aura la possibiliter dans cette partie de gérer :

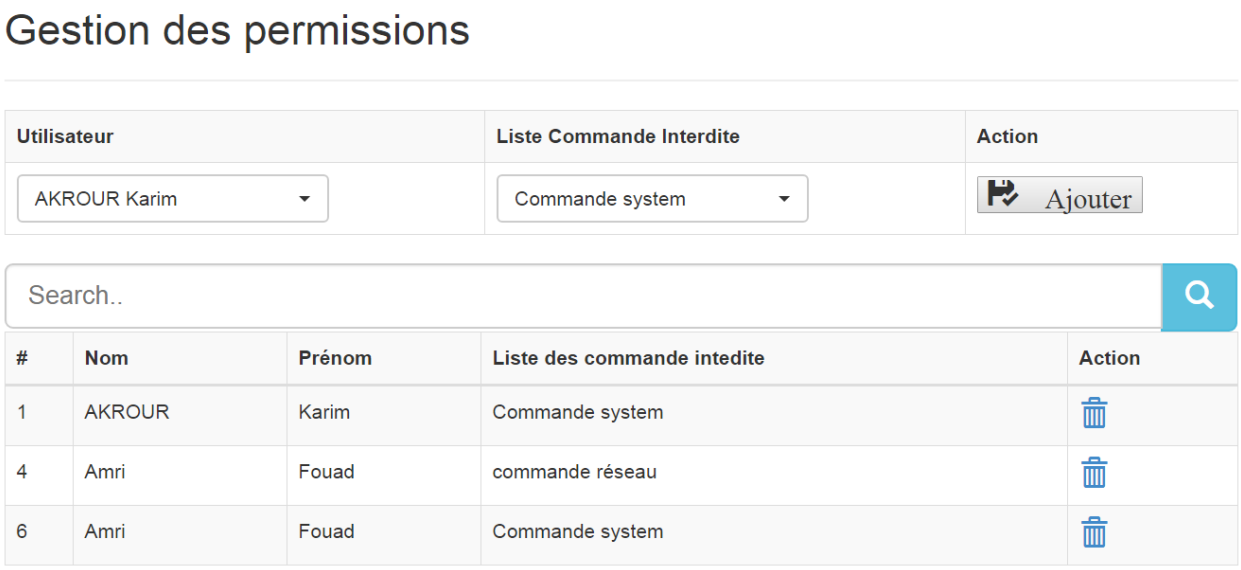


Figure 56 : Interface gestion des permissions.

- **Ajouter une permission :** l'administrateur choisie dans les menus déroulante l'utilisateur et la liste de commande interdite et clique sur le bouton ajouter.
- **Supprimer une permission :** l'administrateur peut supprimer une liste de commande en cliquant sur le bouton une interface de confirmation sera afficher.

3.1.2- Interface Auditeur

❖ **Session SSH**

Dans cette partie l'auditeur peut consulter les connexions des utilisateurs au ressource via le protocole SSH.

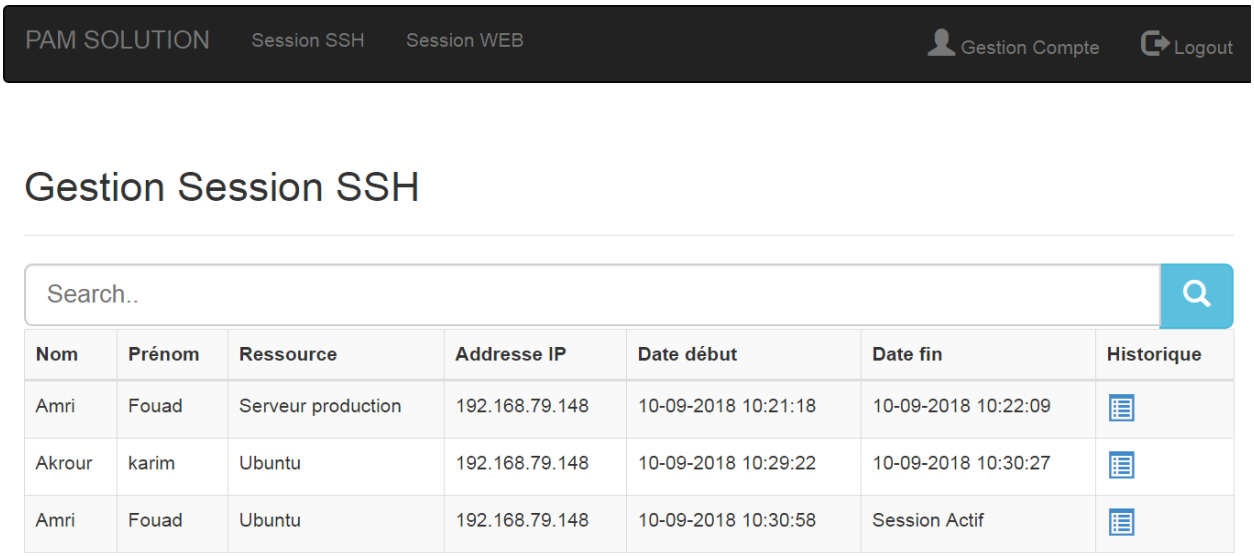


Figure 57 : Interface gestion des sessions SSH.

En cliquant sur le bouton  l'auditeur peut consulter les fichiers log des sessions.

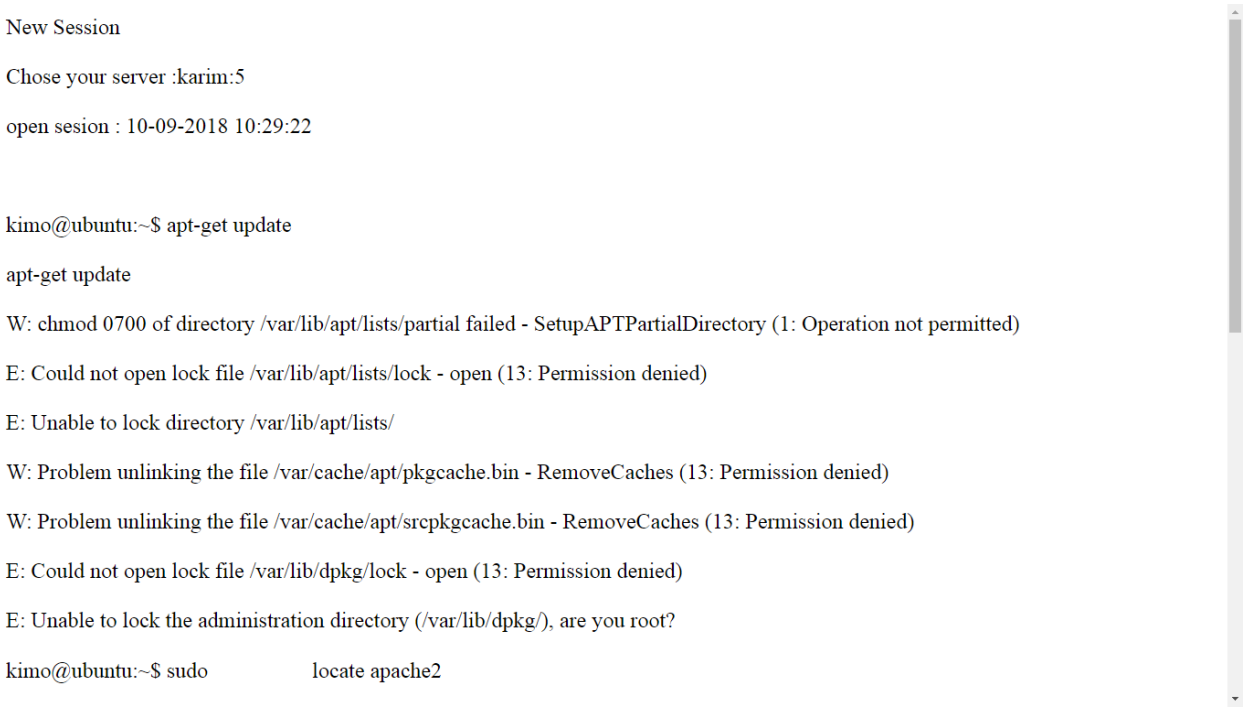


Figure 58 : Consultation fichier log d'une session SSH.

❖ Session WEB

Dans cette partie l'auditeur peut consulter les connexions des administrateurs a l'application WEB.

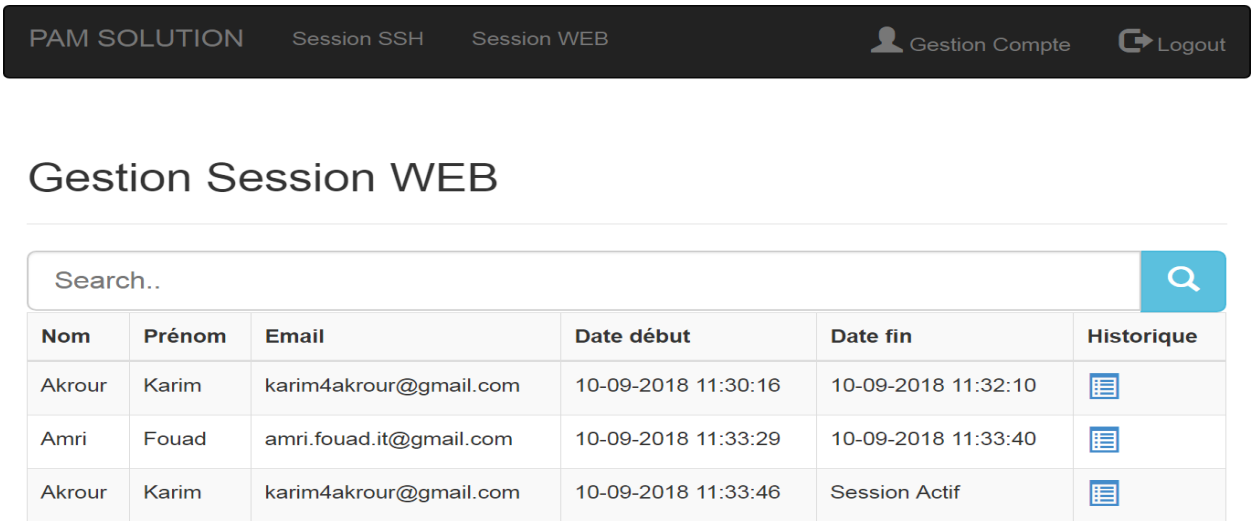


Figure 59: Gestion des sessions WEB.

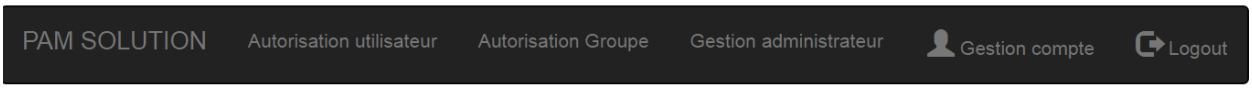
De même que pour les session SSH, l'auditeur peut consulter les fichiers log des sessions en cliquant sur le bouton . 

Figure 60 : Consultation de l'historique d'une session web.

3.1.3- Interface validateur

❖ Autorisation utilisateur

Dans cette partie le validateur aura la possibilité de géré les autorisations des utilisateurs il peut accéder à cette partie en choisissant dans le menu de navigation « Autorisation utilisateur », il aura la possibilité d'effectuer les opérations suivantes :



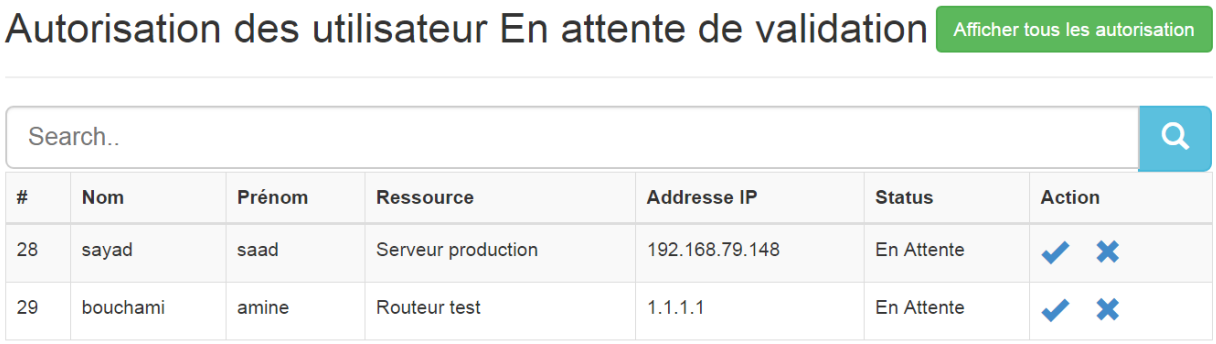


Figure 61: Interface du validateur autorisation utilisateur.

- **Consulter les autorisation utilisateur** : le validateur aura la possibilité de consulter tous les autorisations utilisateur en cliquant sur le bouton afficher autorisation l'interface suivante sera donc afficher

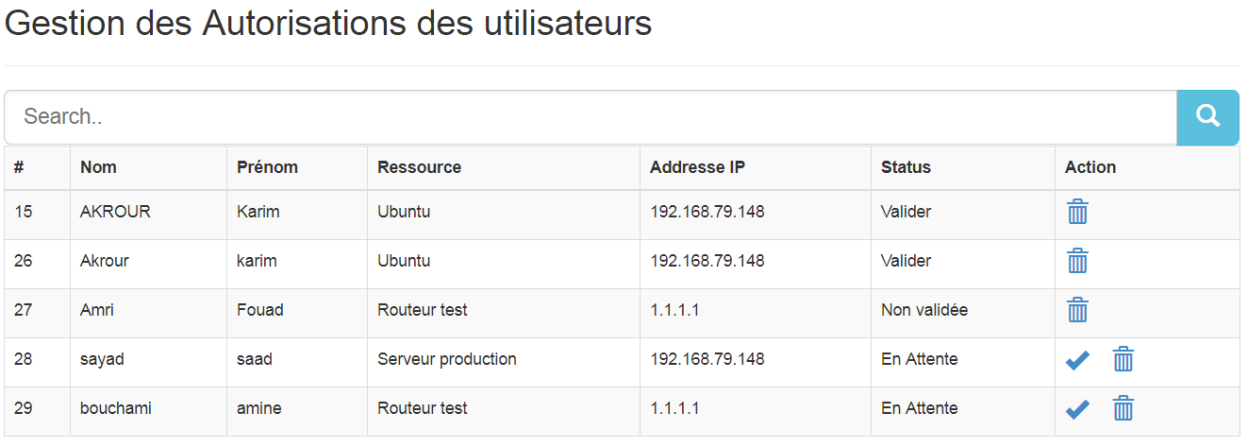


Figure 62 : Interface gestion des autorisation des utilisateur <<Auditeur>>.

- **Approuver une autorisation :** le validateur pourra approuver une autorisation en cliquant sur le bouton , une interface de confirmation sera afficher.
  Une fois le validateur à approuver l'autorisation son statut deviendra « Valider », un email est envoyé à l'administrateur lui notifiant la validation.

Figure 63 : Interface de confirmation valider autorisation.

- Désapprouver une autorisation : le validateur pourra désapprouver une autorisation en cliquant sur le bouton ,une interface de confirmation sera afficher.
  Une fois le validateur a désapprouver l'autorisation son statut deviendra « Non validée », un email est envoyé à l'administrateur lui notifiant la désapprouvassions.

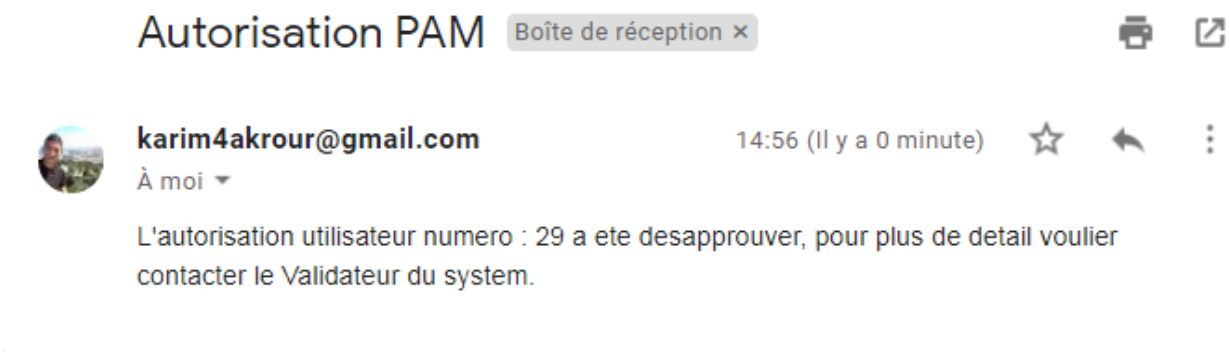


Figure 64 : Exemple d'une notification par email pour les autorisations.

❖ Autorisation groupe

Dans cette partie le validateur aura la possibilité de géré les autorisations des utilisateurs il peut accéder à cette partie en choisissant dans le menu de navigation « Autorisation utilisateur »,

l'interface d'autorisation groupe est similaire à celle de l'autorisation utilisateur, le validateur peut effectuer les mêmes opérations « Consulter les autorisations, Approuver une autorisation, Désapprouver une autorisation ».

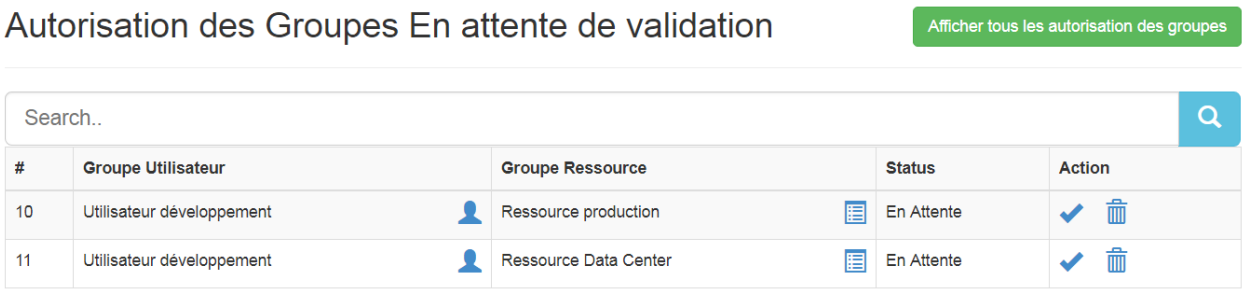


Figure 65 : Interface des autorisation des groupe en attente de validation.

Pour facilité sa tache le validateur aura la possbilité avant d'approuver ou désapprouver une autorisation groupe de :

- Consulter les utilisateurs d'un groupe utilisateur en cliquant sur le bouton qui se trouve à côté de chaque Nom du groupe d'utilisateur, une interface contenant les utilisateurs du groupe sera afficher, alors le validateur pourra vérifier si tous ces utilisateurs on le droit d'accéder à ces ressources avant d'approuver l'autorisation.
- Consulter les ressources d'un groupe ressource en cliquant sur le bouton qui se trouve à côté de chaque Nom du groupe de ressource, de même une interface contenant les ressources du groupe sera affichée.

3.2- Partie serveur proxy « SSH »

Cette partie sera consacré à la réalisation de notre serveur proxy qui sera divisée en deux sous-partie, une pour le serveur et l'autre pour le client (dans notre cas se sont les utilisateur).

Les deux sous-partie sont implémenté avec « Python » dans un même fichier.

L'utilisateur utilise un client SSH « Xshell,PuTTY… » pour se connecter à notre serveur proxy, pour établir une connexion il doit fournir l'adresse IP et le port de notre proxy.

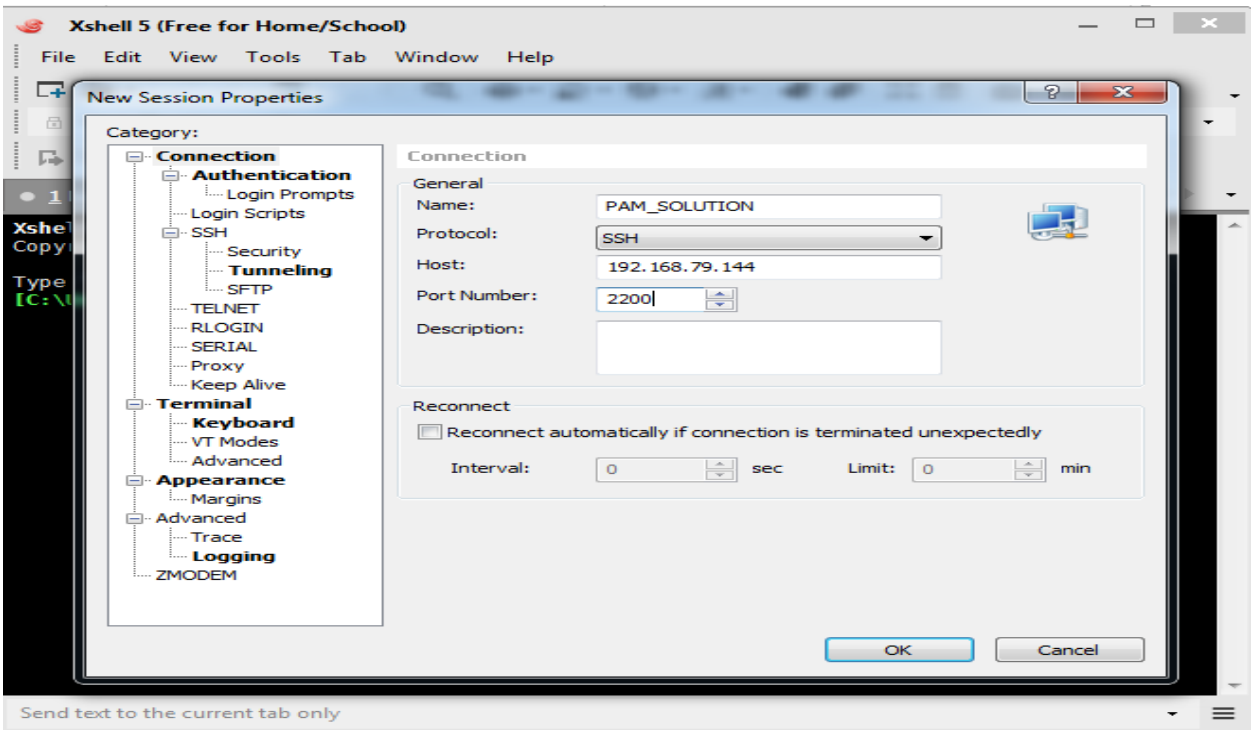


Figure 66 : Interface client SSH <<Xshell>.

Dans notre cas l'adresse du serveur proxy est « 192.168.79.144 » et le port « 2200 », comme notre proxy est de type SSH en utilise donc le même protocole pour se connecté.

Une fois l'utilisateur connecté au proxy, il lui sera demander de fournir ces identifiant « Username » et « Password ».

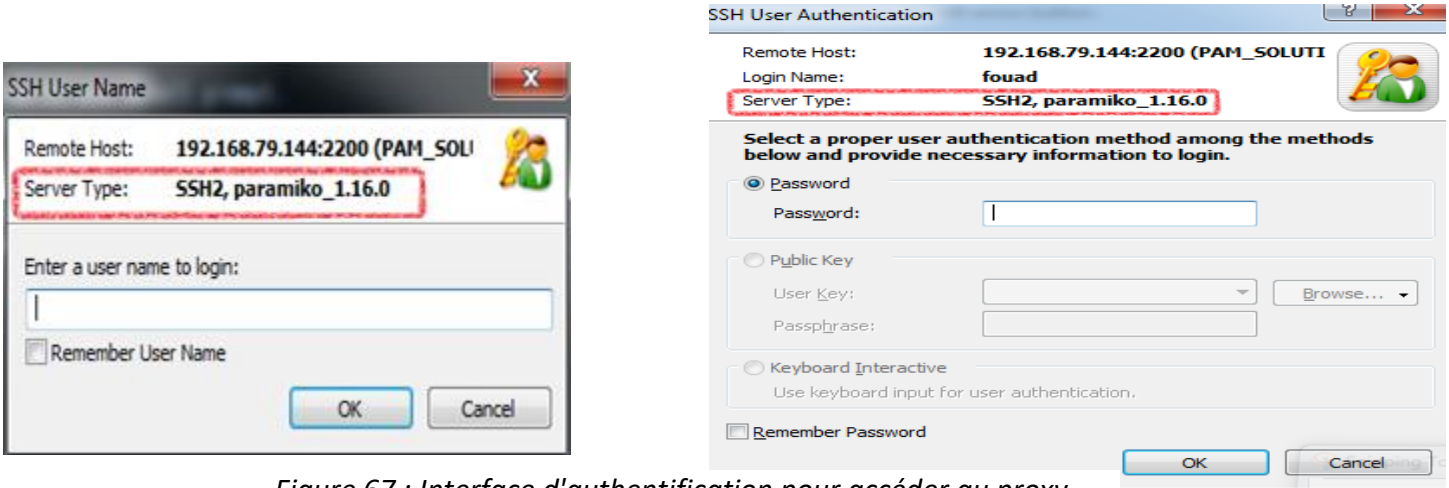


Figure 67 : Interface d'authentification pour accéder au proxy.

En peut voir que le type du server est : « SSH2, paramiko_1.16.0 » donc la connexion sera sécurisée par des formules cryptographique, pour cela le serveur utilise la notion de cryptographie asymétrique, il envoie sa clé publique au utilisateurs pour qu'il l'utilise pour chiffrer leur information et les envoyer au proxy, ce dernier va utiliser sa clé privée pour déchiffré ces informations et les comparé avec la base de donnée afin d'authentifier ces utilisateurs.

Exemple Clé publique : c'est une clé RSA elle est générée par la fonction suivante :

```
# 'data' est le résultas de la fonctions base64.b64encode(key)

data = (b'AAAAB3NzaC1yc2EAAAABIwAAAIEAyO4it3fHlmGZWJaGrfeHOVY7RWO3P9M7hp'
        b'fAu7jJ2d7eothvfeuoRFtJwhUmZDluRdFyhFY/hFAh76PJKGAusIqIQKlkJxMC'
        b'KDqIexkgHAfID/6mqvmnSJf0b5W8v5h2pI/stOSwTQ+pxVhwJ9ctYDhRSlF0iT'
        b'UWT10hcuO4Ks8=')
pub_key = paramiko.RSAKey(data=decodebytes(data))
```

Figure 68 : Exemple de génération d'une clé public RSA avec PARAMIKO.

Après avoir authentifier l'utilisateur, le serveur proxy recherche est affiche tous les ressources autorisées de cet utilisateur et des groupes utilisateurs aux qu'elles il appartient.

En peut voir dans la figure suivante que l'utilisateur « *Amri fouad* » appartient au groupe *« Utilisateur Data Center »*

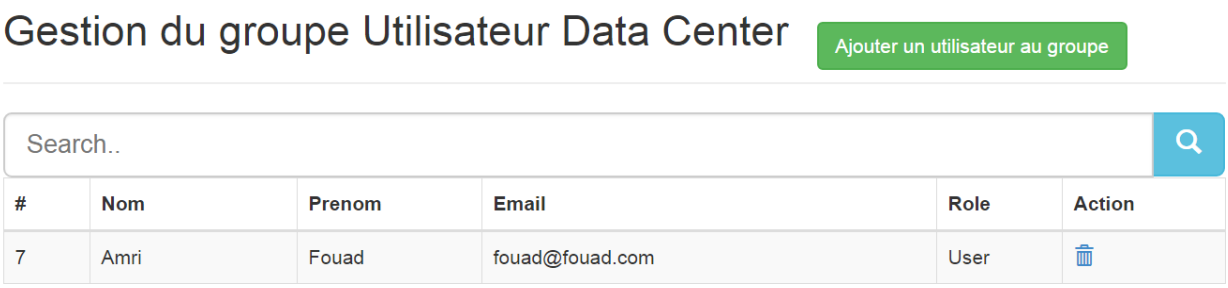


Figure 69 : Exemple d'utilisateur d'un groupe.

Et que ce groupe est autoriser à accéder aux ressource suivante :

Ressource autoriser pour le Groupe Utilisateur Data Center

Search..

#	Nom	Type	Address	Port	Action
7	Serveur production	Serveur	192.168.79.148	22	
5	Ubuntu	Serveur	192.168.79.148	22	

Figure 70 :Exemple d'une liste de ressource autoriser pour un groupe d'utilisateur.

En plus cet utilisateur a une autorisation individuelle pour accéder à la ressource Routeur test mais qui n'est pas encore approuvé par le Validateur.

27	Amri	Fouad	Routeur test	1.1.1.1	En Attente	

Figure 71 : Exemple d'une autorisation en attente de validation.

Donc le serveur proxy va lui afficher seulement les ressources suivantes :

```
Xshell 5 (Build 0446)
Copyright (c) 2002-2014 NetSarang Computer, Inc. All rights reserved.

Type `help' to learn how to use Xshell prompt.
[C:\Users\STALINGRAD]$

Connecting to 192.168.79.144:2200...
Connection established.
To escape to local shell, press 'Ctrl+Alt+]'.

Welcome to PAM SOLUTION  :     Amri Fouad
The list of Resource :
7 :  Serveur production
5 :  Ubuntu
Chose your server :
```

Figure 72 :Interface du proxy à l'étape ou l'utilisateur choisie la ressource cible.

A cette étape l'utilisateur choisie le numéro de la ressource de celle qu'il veut accéder.

Le serveur proxy recherche dans la base de donnée les informations relatif a cette ressource « Adresse IP, Port, Username, Password », et essaye d'ouvrir une session avec cette ressource en utilisant les fonctionnalités de la bibliothèque « *PARAMIKO* ».

```
client = paramiko.SSHClient()
client.load_system_host_keys()
client.set_missing_host_key_policy(paramiko.WarningPolicy())
client.connect(hostname=ip, port=port, username=nom_serveur, password=password_server)
self.shell = client.invoke_shell()
date_open=datetime.now()
```

Figure 73 : Code source pour initialisé une session SSH.

Donc le serveur proxy va ouvrir un « Shell » pour l'utilisateur pour qu'il puisse travailler sur la ressource cible qu'il a choisie.

```
Welcome to PAM SOLUTION  :     Amri Fouad
The list of Resource :
7 :  Serveur production
5 :  Ubuntu
Chose your server :
Open session with :Serveur production Server
 Welcome to Ubuntu 16.04.1 LTS (GNU/Linux 4.4.0-134-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/advantage

351 packages can be updated.
0 updates are security updates.

New release '18.04.1 LTS' available.
Run 'do-release-upgrade' to upgrade to it.

Last login: Tue Sep 11 03:42:54 2018 from 192.168.79.144
kimo@ubuntu:~$
kimo@ubuntu:~$
```

Figure 74: Ouverture d'une session SHELL pour l'utilisateur sur la ressource cible.

Lors de sa session de travaille sur les ressources l'utilisateur sera restreint d'exécuter certaine commande sensible qu'ils lui sont affecté par l'administrateur, autrement dit tous ce que

l'utilisateur exécute sur une ressource est contrôler par notre serveur proxy voici un exemple d'exécution d'une commande interdite.

```
Last login: Tue Sep 11 04:14:34 2018 from 192.168.79.144
kimo@ubuntu:~$
kimo@ubuntu:~$ You can't use this command
```

Figure 75 : Exemple d'exécution d'une commande interdite.

Ce que nous venons d'expliquer est le scénario normal d'une connexion entre un utilisateur et notre proxy sachant que parmi les buts pour lesquels on a développé ce proxy on a la notion de la centralisation qui veux dire que tous les employés doivent passer par le proxy ce qui implique que leurs demandes de connexion peuvent se faire en même temps. Pour remédier à ce problème on a appliqué le principe du « *Multithreading* » de cette façon : le proxy dans son état active va attendre les demandes des connexions, dès qu'il reçoit une demande de connexion il initialise un 'thread' qui va s'occupé de cette demande (assurer l'authentification de cette utilisateur et faire le traitement nécessaire selon les demandes de l'utilisateur) alors que le proxy continu son exécution (écouter des tentatives de connexion des autres utilisateurs) et s'il reçoit une autre demande il initialise un autre 'thread' et c'est ainsi que notre proxy fonctionne.

L'initialisation du thread se fait à travers la fonction suivante :

```
try:
    def __init__(self,host,port):
 self.host=host
 self.port=port
        self.sock = socket.socket(socket.AF_INET, socket.SOCK_STREAM)
        self.sock.setsockopt(socket.SOL_SOCKET, socket.SO_REUSEADDR, 1)
        self. sock.bind((self.host,self.port))
```

Figure 76 : Code d'initialisation d'un THREAD.

La fonction qui va permettre au proxy d'écouter les demandes de connexion est la suivante :

```
try:
    def listen(self):
        self.sock.listen(1000)
        print('Listening for connection ...')
        while True:
            clients, address = self.sock.accept()
            clients.settimeout(60)
            threading.Thread(target = self.listenToClient,args = (clients,address)).start()
```

Figure 77: Code source du proxy pour écouter les demandes de connexion.

Et voici un exemple qui montre l'exécution de plusieurs clients en même temps :

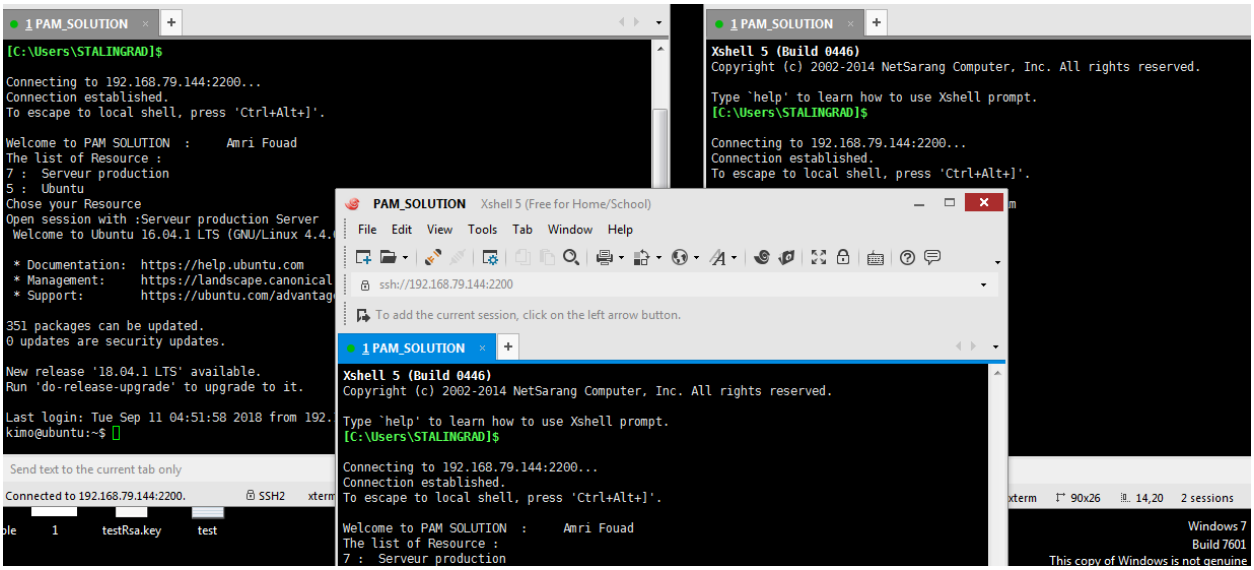


Figure 78 : Exemple d'exécution de plusieurs client en même temps.

Conclusion

A travers ce chapitre, nous avons présenté la réalisation de notre solution en justifiant nos choix technologiques et représentant quelques interfaces graphiques que nous avons jugé les plus importantes.

Conclusion Générale

Le recours aux technologies de l'information et des communications s'avère incontournable dans un contexte caractérisé par une évolution croissante des besoins d'affaires et la production de données volumineuses et parfois sensibles.

Cette situation fait constamment apparaître de nouvelles menaces et de nouvelles situations de vulnérabilités susceptibles de mettre en péril la sécurité de l'information des organisations. De ce fait, l'information est exposée à de nombreux risques qu'il faut réduire à un niveau acceptable par la mise en place de mesures de sécurité, dont la gestion des droits et des privilèges d'accès.

Ce présent rapport a été réalisé dans le but concevoir et réaliser une solution pour remédier à ce type de menaces, notre solution proposée repend totalement aux exigences demandées par l'organisme d'accueil en terme de centralisation des gestions de ces accès et de rependre aux points suivantes :

1. Qui a accès à quelle information?
2. Qui a approuvé l'accès?
3. L'accès est-il adapté aux tâches à accomplir?
4. L'accès et les opérations en découlant sont-ils correctement surveillés, consignés et enregistrés?

En ce fondant sur le principe du « moindre privilège » et de « séparation des taches ».

Nous avant commencer ce rapport par une étude sur les accès privilégiés, ensuite nous avons entamé la partie d'analyse et spécification des besoins ou nous avions bien étudiez les besoins de l'organisme d'accueil le tout en se fixant sur un périmètre de travail qui consiste à un contrôle centralisé des accès des employés de la société aux ressources de leur DATA CENTER via le protocole SSH, sans que ces employés ne changent leur méthode de travail.

Notre solution proposée se base sur l'intégration d'un serveur proxy SSH en utilisant la puissance du langage de script Python et ces différentes bibliothèques qui nous ont permis un

contrôle centralisé sur les accès de ces employés, et à développer une partie web pour faciliter la tâche de l'administrateur.

En termes de sécurité notre solution repose sur plusieurs mécanismes tels que le SSO, le cryptage des sessions entre les utilisateurs et le proxy, et entre le proxy et les ressources cible en utilisant le protocole SSH.

Nous envisagions plusieurs nouvelles fonctionnalités pour notre solution :

- La prise en charge des protocoles : RDP, VNC, HTTPS.
- Le support des différent type d'authentification tel-que : RADIUS, certificat x509.
- Sécurisé l'accès en utilisant l'authentification multi-facteur.
- La visualisation en temps réel des sessions actives.

Bibliographie

[1] Gestion des identités et des accès, *Guide pratique d'audit des technologies de l'information*, The Institute of Internal Auditors, Novembre 2007.

[2] Trois bonne raisons pour une gestion de l'identité des comptes privilégiés, ENTREPRISE MANAGEMENT ASSOCIATE (EMA), février 2015.

[3] CYBERARK, Livre Blanc, THE CYBERARK PRIVILEGED ACCESS SECURITY SOLUTION.

[4] Les comptes à privilèges, un maillon faible de la sécurité du système d'information, poster sur https://www.securityinsider-wavestone.com/2015/03/les-comptes-privileges-un-maillon.html, Consulter le 12/9/2018 à 23.21.

[5] BeyondTrust, External Attacks and privileged accounts, 5 steps to control the threat potential, Nick Cavalancia (Technical Evangelist, Microsoft MVP, & CEO of Conversational Geek).

[6] Identity and Access Management Model, Identity Management Institute, poster sur

https://www.identitymanagementinstitute.org/identity-and-access-management-model/.

consulté le 12/9/2018 à 23.30.

[7] ARE PRIVILEGED ACCESS MANAGEMENT (PAM) AND IDENTITY & ACCESS MANAGEMENT (IAM) THE SAME? , poster le 16 Janvier 2018 par Andy Harris, poster sur: https://osirium.com/blogfeed/privileged-access-management-and-identity-access-management/, consulté le 12/9/2018 à 11:35.

[8] The Forrester Wave, Privileged Identity Management, Andras Cser, Juin 2016.

[9] Verizon, Data Breach Investigations Report, Avril 2017.

[10] Thycotic, State of Privileged Account Management Report, Juillet 2016.

[11] Solution Review, Privileged Access Management Buyer's guide, 2018.

[12] INDIANA UNIVERSITY, About proxy servers, sur https://kb.iu.edu/d/ahoo, consulté le 12/9/2018 à 11:44.

[13] Understanding the SSH Encryption and Connection Process, poster sur https://www.digitalocean.com/community/tutorials/understanding-the-ssh-encryption-and-connection-process, consulter le 12/9/2018 à 11:49.

[14] Un annuaire Active Directory, pourquoi ?, poster **sur** https://www.it-connect.fr/chapitres/un-annuaire-active-directory-pourquoi/, consulté le 18/09/2018 a 15:36.

[15] PHP, https://fr.wikipedia.org/wiki/PHP, consulter le 13/9/2018 à 00.00.

[16] PHP - Connexion à un annuaire LDAP, poster sur https://www.commentcamarche.com/contents/798-php-connexion-a-un-annuaire-ldap, consulter le 18/09/2018 à 15:55.

[17] PHP Mailer, https://fr.wikipedia.org/wiki/PHPMailer, consulter le 13/9/2018 à 00.04.

[18] Bootstrap(Framework), https://fr.wikipedia.org/wiki/Bootstrap_(framework), consulter le 18/09/2018 à 16:19.

[19] Apache Web Server, https://www.techopedia.com/definition/4851/apache-web-server, consulter le 16:25.

[20] Programmation python/introduction, https://fr.wikibooks.org/wiki/Programmation_Python/Introduction, consulter le 18/09/2018 à 16:33.

[21] Paramiko, https://github.com/paramiko/paramiko/, consulter 18/09/2018 à 16:38.

[22] Python – Network Programming**,** https://www.tutorialspoint.com/python/python_networking.html, consulter le 18/09/2018 à 17:16.

[23] Xshell 6, https://www.netsarang.com/products/xsh_overview.html, consulter le 18/09/2018 a 17:18.

[24] MySQL, https://fr.wikipedia.org/wiki/MySQL, consulter le 18/09/2018 à 17:20.

[25] VMware Workstation Pro, https://fr.wikipedia.org/wiki/VMware_Workstation_Pro, consulter le 18/09/2018 a 17:26.

[25] Symmetric vs. Asymmetric Encryption – What are differences?, poster sur https://www.ssl2buy.com/wiki/symmetric-vs-asymmetric-encryption-what-are-differences, Consulter le 22/9/2018.