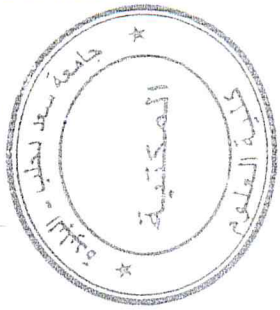
REPUBLIQUE ALGERIENNE DEMOCRATIQUE ET POPULAIRE

MINISTERE DE L'ENSEIGNEMENT SUPERIEUR
ET DE LA RECHERCHE SCIENTIFIQUE



UNIVERSITE SAAD DAHLAB DE BLIDA

FACULTE DES SCIENCES

DEPARTEMENT D'INFORMATIQUE

MEMOIRE DE FIN D'ETUDES

POUR L'OBTENSION DU DIPLÔME

DE MASTER EN INFORMATIQUE

Conception et réalisation d'un système de surveillance des ressources partagées sur un réseau local

Présenté par :

Mr EL ARBI RABAH TOUFIK

Promotrice :
M^me^ REZZOUG Nachida

Encadreur :
Mr ZATOUT Mohamed

Promotion : 2011 – 2012

Dédicaces

Je dédie ce modeste travail

A mes très chers parents, pour leur soutien ; ma mère qui n'a pas cessé de prier

Pour moi et de m'encourager dans les moments difficiles. Mon père qui s'est

Sacrifié afin que rien n'entrave le déroulement de mes études,

A mes grands-mères

A mes frères

A tous mes amis qui m'ont soutenu et encouragé

A toute ma famille

A tous les élèves de la promotion 2012

SOMMAIRE

LISTE DES FIGURES

LISTE DES TABLEAUX

Introduction générale

Au sein d'une entreprise, les utilisateurs du réseau informatique ne sont pas forcement des informaticiens, d'où les risques de manipulations non-intentionnelles : partage de documents classifiés, transfert de documents vers une station inconnue,...etc. En absence d'un outil professionnel de surveillance réseau, cette tâche devient très importante (voir pénible) pour l'administrateur (exécution de lignes de commandes, parcours du réseau, ... etc.), d' où l'objet du présent travail.

A l'issu de ce travail, l'utilisateur avancé (ou l'administrateur) d'un réseau local *Microsoft*, disposera d'un outil qui lui permettra de connaître à tout instant les ressources partagées (type de ressource, accès aux ressources, utilisateurs courants,...etc.) et prendre les décisions nécessaire à l'encontre des failles et problèmes observés.

L'objectif est donc de développer un outil de surveillance des ressources partagées sur un LAN dont on maîtrise son fonctionnement en étant à l'origine de ses programmes sources, contrairement à un outil commercialisé (propriétaire) qui est souvent qu'un ensemble de fichiers binaires non accessibles aux développeurs .

Pour présenter notre travail, le mémoire a été structuré comme suit :

- Un premier chapitre on a effectue une étude théorique des notions réseaux telle que la décomposition standard des différentes couches OSI, l'architecture d'un système client/server, les déférents protocoles employés et matériels utilisé et ça configuration.
- Un deuxième chapitre on a présenté des logiciels de la supervision réseau, ces objectifs et principes, et une présentation de Protocol SNMP ces avantages, inconvénients etc.
- Le troisième chapitre présenté par la conception porte sur l'architecture globale ainsi que la conception de l'ensemble des composantes de l'outil de surveillance des ressources partagées on utilisant le langage UML.
- Pour le dernier chapitre présenté par l'implémentation on traite l'environnement sur lequel ces composants ont été développés ainsi que l'implémentation des différents modules logiciels constituant notre outil. Finalement en termine par une conclusion générale.

Chapitre I

Introduction aux réseaux

Ce chapitre nous aborderons les grands principes régissant les équipements matériels et logiciels permettant d'échanger des données mises sous forme numérique et qui forment les réseaux informatiques.

I. Introduction

Les réseaux informatiques qui permettaient à leur origine de relier des terminaux passifs à de gros ordinateurs centraux autorisent à l'heure actuelle l'interconnexion de tous types, d'ordinateurs que ce soit de gros serveurs, des stations de travail, des ordinateurs personnels ou de simples terminaux graphiques. Les services qu'ils offrent font partie de la vie courante des entreprises et administrations (banques, gestion, commerce, bases de données, recherche, etc.) et des particuliers (messagerie, loisirs, services d'informations par minitel et Internet...).

II. Avantages d'un réseau

Maintient de la chaine numérique entre les ordinateurs : les fichiers informatiques sont échangés de poste à poste sans recourir a un support intermédiaire : cd-rom, clé USB…

Partage des ressources matériels et logiciels : les périphériques (imprimante, scanner, modem), les applications, les accès internet sont mise en commun ; ce qui réduit les investissements et des couts de maintenance.

Partage des fichiers : (base de données ou autre) permet à plusieurs utilisateurs de consulter simultanément un fichier identique et unique. A contrario cela évité la dissémination et les doublons de fichiers son synchronisés. (Exemple : un fichier est copulé sur plusieurs ordinateurs et les mises à jour ne sont plus répercutées dans le fichier initial)

Favorise le travail collaboratif : la mise en œuvre de messageries internes ou externes, d'agendas communs, d'espaces de travail partagés facilite les échanges et les communications.

Sécurisation et confidentialité : le système d'exploitation du serveur permet de paramétrer des contrôles d'accès au réseau et aux ressources par des comptes d'utilisateurs ou des groupes et des mots de passe.

Automatisation des sauvegardes : il est possible de paramétrer des sauvegardes des centralisé, régulières et automatiques qui protègent contre les accédants.

Installation et paramétrages des postes à partir du serveur : les installations, paramétrages des contrôles sont centralisés, ce qui les rend plus rapides à mettre en œuvre et améliore la sécurité du système informatique.

Complexité : un réseau est plus complexe à administrer et à gérer qu'un ordinateur individuel. Son administration doit obligatoirement être confiée à un spécialiste. Par ailleurs, les pannes sont très perturbantes pour l'organisation car tous les postes du réseau en sont victimes.

Coût : la mise en œuvre d'un réseau génère des coûts d'installation matériels, de paramétrages des sécurités et de maintenance qui peuvent être importants pour les entreprises.

Dépersonnalisation des échanges : le réseau facilite la communication mais ces échanges peuvent conduire à une déshumanisation des rapports qui passent par des machines.

III. Les couches réseau modèle OSI

Au début des années 70, chaque constructeur a développé sa propre solution réseau autour d'architecture et de protocoles privés (SNA d'IBM, DECnet de DEC, DSA de Bull, TCP/IP du DoD,...) et il s'est vite avéré qu'il serait impossible d'interconnecter ces différents réseaux « propriétaires » si une norme internationale n'était pas établie. Cette norme établie par l'International Standard Organization (ISO) est la norme Open System Interconnection (OSI, interconnexion de systèmes ouverts). Un système ouvert est un ordinateur, un terminal, un réseau, n'importe quel équipement respectant cette norme et donc apte à échanger des informations avec d'autres équipements hétérogènes et issus de constructeurs différents.

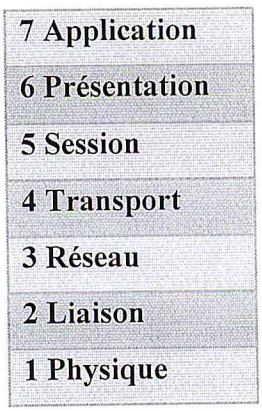


Fig.1 Les sept couches de modèle de référence OSI de l'ISO

Le premier objectif de la norme OSI a été de définir un modèle de toute architecture de réseau basé sur un découpage en sept couches (cf. figure 1), chacune de ces couches correspondant à une fonctionnalité particulière d'un réseau. Les couches 1, 2, 3 et 4 sont dites basses et les couches 5, 6 et 7 sont dites hautes.

Une couche assurant la transmission de l'application demandée avec envoie de messages.	**7**	Couche application	Gère les applications de types réseaux : courrier électronique, transfert de fichier, appel de procédure distante…
	6	Couche présentation	Assure une transparence en terme de codage (ex. ASCII).
	5	Couche session	S'occupe de fiabiliser la communication utilisateurs, gère des tours de parole, synchronisation.
Une couche de communication de base permettant de transmettre physiquement en respectant un certain nombre de règles.	**4**	Couche transport	Optimise l'utilisation de la couche réseau et assure des travaux de type fragmentation de message (ex. TCP).
	3	Couche réseau	Offre un nombre de services dont un service d'adressage (IP) permettant d'atteindre son destinataire, un service de routages déterminant un chemin à l'intérieur du réseau maillé et un contrôle du flux pour ne pas saturer le réseau.
	2	Couche liaison de données	Permet d'assurer une liaison fiable par une bonne synchronisation et une détection d'erreurs.
	1	Couche physique	Emet des signaux assurant la bonne transmission.

Tab.1. Les sept couches de modèle de référence OSI de l'ISO

IV. Présentation d'un réseau local

Le réseau local, en anglais LAN (Local Area Network) ou en français RLE (Réseau Local d'Entreprise), est une infrastructure de communications reliant des équipements informatiques et permettant de partager des ressources communes sur une aire limitée à quelques centaines de mètres.

IV.1. Caractéristiques du réseau local

Les réseaux locaux sont des infrastructures complexes et pas seulement des câbles entre stations de travail. Et, si l'on énumère la liste des composants d'un réseau local, on sera peut-être surpris d'en trouver une quantité plus grande que prévue :

* La **méthode d'accès** décrit la façon dont le réseau arbitre les communications des différentes stations sur le câble : ordre, temps de parole, organisation des messages. Elle dépend étroitement de

la topologie et donc de l'organisation spatiale des stations les unes par rapport aux autres. La méthode d'accès est essentiellement matérialisée dans les cartes d'interfaces, qui connectent les stations au câble.

* Les **protocoles** de réseaux sont des logiciels qui "tournent" à la fois sur les différentes stations et leurs cartes d'interfaces réseaux.

* Le **système d'exploitation** du réseau (ou NOS pour Network Operating System), souvent nommé gestionnaire du réseau, réside dans les différentes stations du réseau local. Il fournit une interface entre les applications de l'utilisateur et les fonctions du réseau local auxquelles il fait appel par des demandes à travers la carte d'interface.

* Le ou les **serveurs de fichiers** stocke et distribue les fichiers de programmes ou les données partageables par les utilisateurs du réseau local. Il résulte d'une combinaison de matériel et de logiciel qui peut être spécifique.

* Le **système de sauvegarde** est un élément indispensable qui fonctionne de diverses manières soit en recopiant systématiquement tous les fichiers du ou des serveurs, soit en faisant des sauvegardes régulières, éventuellement automatisées.

* Les **ponts**, les **routeurs** ou les **passerelles** constituent les moyens de communication qui permettent à un de ses utilisateurs de " sortir " du réseau local pour atteindre d'autres réseaux locaux ou des serveurs distants.

* Le **système de gestion et d'administration** du réseau envoie les alarmes en cas d'incidents, comptabilise le trafic, mémorise l'activité du réseau et aide le superviseur à prévoir l'évolution de son réseau. [5]

IV.2. Le câblage

Le câblage des réseaux locaux tend aujourd'hui à se banaliser, et à ne pas se distinguer du câblage informatique et téléphonique général de l'entreprise. Trois médias sont aujourd'hui utilisés dans les réseaux locaux :

* La **paire torsadée téléphonique**, peu chère, assez facile à poser, elle est aujourd'hui le support le plus répandu pour les réseaux locaux.

* Le **câble coaxial**, nettement plus cher, est en perte de vitesse après avoir été le support par excellence des premiers réseaux locaux qui fonctionnaient en mode large bande (bande passante découpée en plages de fréquence, chacune étant attribuée à un canal). Aujourd'hui, la plupart des réseaux locaux fonctionnant en bande de base (toutes les stations émettent sur un même canal occupant la totalité de la bande passante), le câble coaxial est moins nécessaire et on l'emploie presque uniquement pour l'interconnexion de différents réseaux locaux.

* La **fibre optique**, encore nettement plus chère, parce qu'elle permet des débits élevés et est insensible aux parasites, commence à faire une percée dans les réseaux locaux à gros besoins de bande passante (calcul technique, CAO), mais sert surtout pour interconnecter plusieurs réseaux locaux.

IV.3. La topologie

Il faut distinguer la topologie de câblage de la topologie d'accès : la première représente l'implantation des câbles, la seconde la logique de connexion des stations et donc le cheminement qu'empruntent réellement les signaux.

En matière de topologie physique, on utilise principalement le **bus** et l'**étoile**. Dans un bus, le câble relie les stations directement les unes aux autres, comme un réseau de distribution d'eau. Il faut donc une terminaison à l'extrémité du bus. Une variante du bus est l'arbre qui hiérarchise différents sous-bus comme des branches, autorisant parfois plusieurs chemins pour aller d'une station à l'autre.

Dans l'étoile, les câbles sont tous concentrés en un point central, le **concentrateur** ou **hub**. Souvent, on superpose plusieurs étoiles, l'extrémité d'une branche pouvant être le centre d'une nouvelle étoile de niveau inférieur, on parle alors de **répartiteurs**. C'est ce type de câblage qui est le plus employé, plus facile à configurer et à gérer : on peut facilement ajouter une branche à l'étoile pour relier une nouvelle station.

En matière de topologie d'accès, on trouve le bus, l'étoile et l'anneau.

Les anneaux ne sont jamais câblés comme tels : on emploie un câblage en étoile par paires de fils ; le premier fil d'une paire correspondant à une station est relié, dans le répartiteur, au second fil de la paire de la station voisine, et ainsi de suite pour créer un anneau " logique ".

Les concentrateurs et les répartiteurs ou hubs sont souvent des dispositifs actifs, en pratique des cartes électroniques dans des racks, qui gèrent les raccordements, détectent l'arrivée du signal, les

ruptures... Ils jouent un rôle important dans l'administration du réseau et supportent de plus en plus souvent d'autres équipements (ponts, routeurs...)

V. Présentation de l'architecture d'un système client server

De nombreuses applications fonctionnent selon un environnement client/serveur, cela signifie que des **machines clientes** (des machines faisant partie du réseau) contactent un **serveur**, une machine généralement très puissante en termes de capacités d'entrée-sortie, qui leur fournit des **services**. Ces services sont des programmes fournissant des données telles que l'heure, des fichiers, une connexion, etc. Les services sont exploités par des programmes, appelés **programmes clients**, s'exécutant sur les machines clientes. On parle ainsi de client FTP, client de messagerie, ..., lorsque l'on désigne un programme, tournant sur une machine cliente, capable de traiter des informations qu'il récupère auprès du serveur (dans le cas du client FTP il s'agit de fichiers, tandis que pour le client messagerie il s'agit de courrier électronique).

Dans un environnement purement Client/serveur, les ordinateurs du réseau (les clients) ne peuvent voir que le serveur, c'est un des principaux atouts de ce modèle.

V.1. Avantages de l'architecture client/serveur

Le modèle client/serveur est particulièrement recommandé pour des réseaux nécessitant un grand niveau de fiabilité, ses principaux atouts sont:

- **des ressources centralisées**: étant donné que le serveur est au centre du réseau, il peut gérer des ressources communes à tous les utilisateurs, comme par exemple une base de données centralisée, afin d'éviter les problèmes de redondance et de contradiction
- **une meilleure sécurité**: car le nombre de points d'entrée permettant l'accès aux données est moins important
- **une administration au niveau serveur**: les clients ayant peu d'importance dans ce modèle, ils ont moins besoin d'être administrés
- **un réseau évolutif**: grâce à cette architecture ont peu supprimé ou rajouter des clients sans perturber le fonctionnement du réseau et sans modifications majeures

V.2. Inconvénients du modèle client/serveur

L'architecture client/serveur a tout de même quelques lacunes parmi lesquelles:

- **un coût élevé** dû à la technicité du serveur
- **un maillon faible**: le serveur est le seul maillon faible du réseau client/serveur, étant donné que tout le réseau est architecturé autour de lui! Heureusement, le serveur a une grande tolérance aux pannes (notamment grâce au système RAID)

V.3. Fonctionnement d'un système client/serveur

Un système client/serveur fonctionne selon le schéma suivant:

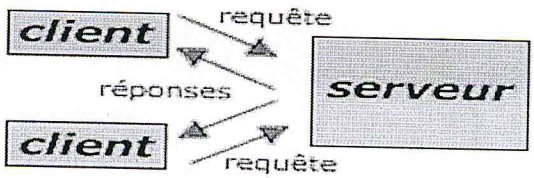


Fig.2 Système client serveur

- Le client émet une requête vers le serveur grâce à son adresse et le port, qui désigne un service particulier du serveur
- Le serveur reçoit la demande et répond à l'aide de l'adresse de la machine client et son port

V.4. Présentation de l'architecture à 2 niveaux

L'architecture à deux niveaux (aussi appelée *architecture 2-tier*, *tier* signifiant *étage* en anglais) caractérise les systèmes clients/serveurs dans lesquels le client demande une ressource et le serveur la lui fournit directement. Cela signifie que le serveur ne fait pas appel à une autre application afin de fournir le service.

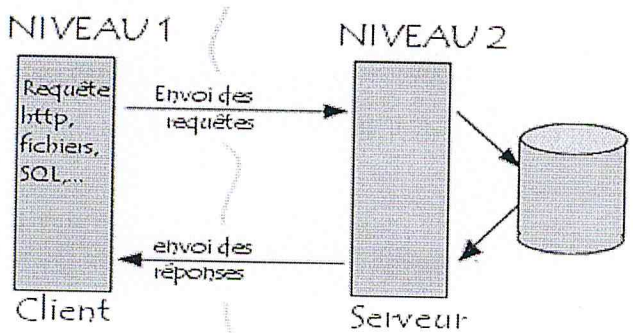


Fig.3. Architecture client serveur a deux niveaux

V.5. Présentation de l'architecture à 3 niveaux

Dans l'architecture à 3 niveaux (appelées *architecture 3-tier*), il existe un niveau intermédiaire, c'est-à-dire que l'on a généralement une architecture partagée entre:

1. Le client: le demandeur de ressources
2. Le serveur d'application (appelé aussi **middleware**): le serveur chargé de fournir la ressource mais faisant appel à un autre serveur
3. Le serveur secondaire (généralement un serveur de base de données), fournissant un service au premier serveur

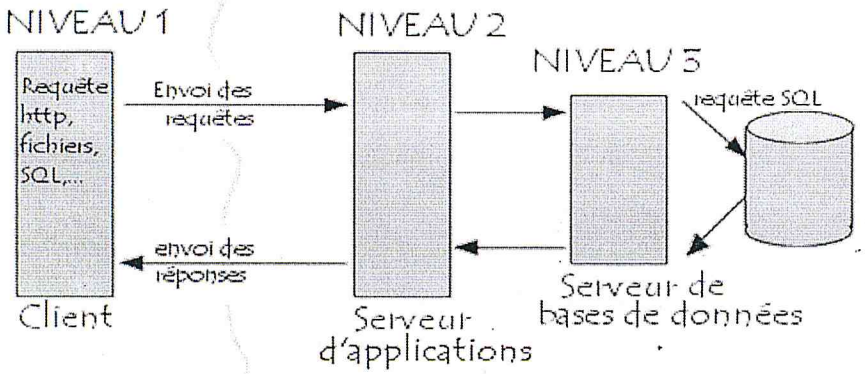


Fig.4. Architecture client a trois niveaux

Etant donné l'emploi massif du terme d'architecture à 3 niveaux, celui-ci peut parfois désigner aussi les architectures suivantes:

- Partage d'application entre client, serveur intermédiaire, et serveur d'entreprise
- Partage d'application entre client, base de données intermédiaire, et base de données d'entreprise

V.6. Comparaison des deux types d'architectures

L'architecture à deux niveaux est donc une architecture client/serveur dans laquelle le serveur est polyvalent, c'est-à-dire qu'il est capable de fournir directement l'ensemble des ressources demandées par le client. Dans l'architecture à trois niveaux par contre, les applications au niveau serveur sont

délocalisées, c'est-à-dire que chaque serveur est spécialisé dans une tâche (serveur web/serveur de base de données par exemple). Ainsi, l'architecture à trois niveaux permet:

- une plus grande flexibilité/souplesse
- une plus grande sécurité (la sécurité peut être définie pour chaque service)
- de meilleures performances (les tâches sont partagées)

V.7. L'architecture multi-niveaux

Dans l'architecture à 3 niveaux, chaque serveur (niveaux 1 et 2) effectue une tâche (un service) spécialisée. Ainsi, un serveur peut utiliser les services d'un ou plusieurs autres serveurs afin de fournir son propre service. Par conséquence, l'architecture à trois niveaux est potentiellement une architecture à N niveaux...

VII. VLAN

Ce n'est pas une nouvelle norme de réseau local mais une méthode pour gérer les réseaux locaux. Il s'agit plus de supervision de réseau.

Les VLAN constituent une étape importante dans la gestion d'un grand réseau. En effet beaucoup de temps est passé pour séparer physiquement les réseaux dans des panneaux de brassage.

En général un grand réseau n'est pas un réseau tout à plat mais une série de réseaux cloisonnées physiquement et interconnectés par des routeurs. Lorsqu'un utilisateur se déplace ou un bureau change d'affectation, il faut se déplacer pour modifier le panneau de brassage de manière à mettre ce bureau sur un autre HUB.

En fait avec les VLAN, qui prennent tout leur poids avec les commutateurs et leur généralisation, il est possible à partir d'une station de supervision de grouper les utilisateurs entre eux sans se déplacer. Le résultat est identique à une séparation physique. On ne pourra pas faire de partage d'information bricolé avec le collègue d'un autre service. [1]

VIII. Introduction à IP (INTERNET PROTOCOL)

VIII.1. Description fonctionnelle

La fonction ou rôle du Protocole Internet est d'acheminer les datagrammes à travers un ensemble de réseaux interconnectés. Ceci est réalisé en transférant les datagrammes d'un module Internet à l'autre jusqu'à atteindre la destination. Les modules Internet sont des programmes exécutés dans des hôtes et des routeurs du réseau Internet. Les datagrammes sont transférés d'un module Internet à l'autre sur

un segment particulier de réseau selon l'interprétation d'une adresse Internet. De ce fait, un des plus importants mécanismes du protocole Internet est la gestion de cette adresse Internet.

Lors de l'acheminement d'un datagramme d'un module Internet vers un autre, les datagrammes peuvent avoir éventuellement à traverser une section de réseau qui admet une taille maximale de paquet inférieure à celle du datagramme. Pour surmonter ce problème, un mécanisme de fragmentation est géré par le protocole Internet.

VIII.2. Adressage

Une distinction doit être faite entre noms, adresses, et chemins. Un nom indique ce que nous cherchons. Une adresse indique où cela se trouve. Un chemin indique comment y aboutir. Le protocole Internet s'occupe essentiellement des adresses. C'est à des protocoles de niveau plus élevé (ex., hôte-vers-hôte ou application) que revient la tâche de lier des noms à des adresses. Le module Internet déduit de l'adresse Internet une adresse réseau local. La tâche qui consiste à transcrire l'adresse de réseau local en termes de chemin (ex., sur un réseau local ou dans un routeur) revient au protocole de bas niveau.

Les adresses ont une longueur fixe de 4 octets (32 bits). Une adresse commence toujours par un numéro de réseau, suivi d'une adresse locale (appelée le champ "reste") codant l'adresse de l'hôte sur ce réseau. Il existe trois formats ou classes d'adresses Internet : pour la classe A, le bit de poids fort vaut zéro, les 7 bits suivants désignent le réseau, les derniers 24 bits désignent l'adresse locale de la machine; pour la classe B, les deux bits de poids fort valent 1 et 0, les 14 bits suivants désignent le réseau et les 16 derniers bits l'adresse locale de machine ; pour la classe C, les trois bits de poids fort forment le schème 110, les 21 bits suivants forment l'adresse réseau et les 8 derniers bits l'adresse locale.

La transcription d'adresse Internet en adresses de réseau local doit être sujette à quelques précautions; un hôte physique unique peut abriter plusieurs adresses Internet distinctes comme s'il s'agissait de plusieurs hôtes indépendants. Certains hôtes peuvent disposer de plusieurs interfaces physiques (multi-homing).

De ce fait, il faudra pouvoir considérer le cas d'un hôte à plusieurs interfaces physiques chacune abritant plusieurs adresses Internet distinctes.

VIII.3. Adresse IP et adresse MAC

Maintenant que nous savons ce qu'on envoie, il faut que le destinataire le reçoive... Cela fonctionne comme une ligne de téléphone : votre voix doit être amenée rapidement vers votre interlocuteur, quelque soit l'endroit du monde où il se trouve... Pour cela, chaque ordinateur à deux adresses : **une adresse IP et une adresse MAC**. L'adresse IP est en quelque sorte **le nom de votre ordinateur sur un réseau**. Avec cette adresse, on peut situer votre ordinateur dans le monde car on sait à quel réseau il appartient. L'adresse MAC est **l'adresse physique de l'ordinateur** : c'est son nom, quelque soit l'endroit où il est. Ainsi, une fois que le réseau est trouvé grâce à l'adresse IP, l'adresse MAC permet d'être repéré de façon unique. On associe donc un nom de réseau (adresse IP) et une adresse sur ce réseau (adresse MAC) pour envoyer les informations au bon destinataire. Ainsi, si quelqu'un veut vous parler, il envoie un message du style "Est-ce que quelqu'un a vu l'ordinateur d'adresse IP xxx.xxx.xxx.xxx?" et vous lui répondez en lui envoyant votre adresse MAC pour qu'il sache physiquement où vous êtes. Ainsi, tout se passe comme quand quelqu'un vous cherche et qu'il ne vous connait pas : il commence par chercher la pièce où vous êtes et demande à voix haute : "Est-ce que X est là?" et vous lui répondez... **[5]**

IX.1. Les hubs

C'est ce qu'il y a de plus simple. Ca se présente comme une petite boîte allongée (genre multiprise en ligne) avec pleins de prises « RJ45 » (mais si, vous voyez bien, c'est les petites prises qu'il y a sur les cartes réseaux) côte à côte. Il y a quand même une prise de courant, mais c'est à peu près tout. Chaque ordinateur est connecté à une des prises.

Les hubs sont souvent utilisés quand il s'agit de relier quelques ordinateurs ensemble pour un petit réseau local. Le principe est simple, dès que quelque chose arrive sur une des prises, il est automatiquement répéter sur toutes les autres prises. C'est pour cela qu'en français, on appelle ça un répéteur...

Ainsi, dès qu'un ordinateur dit quelque chose, tout le monde l'entend et l'ordinateur concerné traite l'information... C'est pour cette raison que ce système ne peut être utilisé que lorsqu'il n'y a que peu d'ordinateurs, car s'il y a 100 ordinateurs qui parlent en même temps et que tout le monde entend tout ce que tout le monde dit, ça devient vite.

XI.2. Les Switchs

Les Switchs sont un peu plus intelligents. C'est déjà un peu plus gros qu'un hub parce qu'on commence à mettre des choses dedans...

Il y a toujours ce principe de prises où sont connectés les différents ordinateurs (mais on peut aussi mettre d'autres Switchs, ou des hubs, ou ce que l'on veut...). La différence avec le hub, c'est que le switch sait quels sont les ordinateurs qui sont autour de lui. Ainsi, s'il reçoit une trame pour l'ordinateur X, il ne l'envoie qu'à l'ordinateur X et pas aux autres. Il commute (il branche) l'entrée des données vers la sortie où est l'ordinateur concerné. C'est pour cela qu'on appelle ça un commutateur en français...

A noter malgré tout que les Switchs font beaucoup de progrès ces temps-ci, ils sont maintenant presque aussi doués que les routeurs (que l'on va voir juste après). Leur fonction première reste quand même celle décrite ci-dessus.

IX.3. Les routeurs

C'est ce que l'on fait de mieux pour acheminer les données. Le routeur est quasiment un ordinateur à part entière. Il est capable de décoder les trames jusqu'à retrouver l'adresse IP et de diriger l'information dans la bonne direction. On peut aussi définir dans les trames le chemin où doit passer la trame, le routeur peut comprendre tout cela... Le fait de définir ou de diriger une trame s'appelle « router » une trame. C'est pour cela qu'on les appelle des routeurs. Ainsi, vous pouvez donner des informations de routage aux informations que vous envoyez

X. Serveur DHCP

Lorsque vous passez par un opérateur quelconque pour vous connecter, il arrive souvent que vous n'avez pas d'adresse IP fixe. En fait, à chaque fois que vous vous connectez, le **serveur DHCP vous attribue une adresse IP pour la connexion** et vous l'enlève quand vous vous déconnectez.

XI. Le Protocol SMB

Ce protocole a été développé par Intel, Microsoft et IBM au début des années 80. C'est ce que Microsoft utilise pour partager ses fichiers et imprimantes dans ses systèmes d'exploitation. Dans l'ancien Windows NT 4, il était appelé **CIFS** (Common Internet File System). Dans Vista et Windows 7, il est appelé SMB

Le protocole SMB (Server Message Block) est un protocole de partage de fichiers réseau qui permet à des applications installées sur un ordinateur d'accéder en lecture et en écriture à des fichiers et de solliciter des services auprès de programmes serveur sur un réseau informatique. Le protocole SMB peut être utilisé en plus du protocole TCP/IP ou d'autres protocoles réseau. Grâce à lui, une application (ou bien l'utilisateur d'une application) peut accéder à des fichiers ou d'autres ressources sur un serveur distant. Les applications peuvent ainsi lire, créer et mettre à jour des fichiers sur le serveur distant. Il permet aussi de communiquer avec n'importe quel programme serveur configuré pour recevoir une demande de client SMB. Windows Server 2012 présente la nouvelle version 3.0 du protocole SMB. [6]

Chapitre II

Supervision réseau

I. Introduction

Actuellement aucune entreprise ne peut se passer d'outils informatiques, et très souvent un réseau informatique de taille plus ou moins importante est mis en œuvre. Le nombre des machines dans ces réseaux peut parfois devenir extrêmement élevé; La maintenance ainsi que la gestion de ces parcs informatiques deviennent alors des enjeux cruciaux, d'autant plus qu'une panne du réseau peut parfois avoir des conséquences catastrophiques.

C'est pourquoi les administrateurs réseau font appel à des logiciels de surveillance et de supervision de réseaux. Ces logiciels vérifient l'état du réseau ainsi que des machines connectées et permettent à l'administrateur d'avoir une vue d'ensemble en temps réel de l'ensemble du parc informatique sous sa responsabilité. Il peut être aussi informé (par email, par SMS) en cas de problème. Grâce à un tel système, les délais d'interventions sont fortement réduits.

II. Présentation

II.1. Objectifs

Il est aujourd'hui de plus en plus difficile d'administrer un réseau. En effet le nombre d'équipements à gérer est souvent important : stations, serveurs, imprimantes... Le plus grand souci d'un administrateur est la panne. En effet, il doit pouvoir réagir le plus rapidement possible pour effectuer les réparations nécessaires. Il faut pouvoir surveiller de manière continu l'état des systèmes d'information afin d'éviter un arrêt de production de trop longue durée. C'est là ou la supervision intervient. Elle doit permettre d'anticiper les problèmes et de faire remonter des informations sur l'état des équipements. Plus le système est important et complexe, plus la supervision devient compliquée sans les outils indispensables.

II.2. Principe

Une grande majorité des logiciels de supervision sont basés sur le protocole SNMP qui existe depuis de nombreuses années. Nous en faisons la description dans la deuxième partie.

La plupart de ces outils permettent de nombreuses fonctions dont voici les principales :

- ✓ Surveiller le système d'information
- ✓ Visualiser l'architecture du système
- ✓ Analyser les problèmes
- ✓ Déclencher des alertes en cas de problèmes
- ✓ Effectuer des actions en fonction des alertes

La tache de l'administrateur est alors simplifiée. Il n'a plus qu'à faire une vérification ou réaliser une action en fonction d'une alerte déclenchée. Chaque outil doit aussi lui donner une vision globale du système d'information pour localiser les problèmes le plus rapidement possible. [2]

III. Le protocole SNMP

III.1.Présentation

SNMP signifie Simple Network Management Protocol (protocole simple de gestion de réseau en Français). C'est un protocole qui permet comme son nom l'indique, de gérer les équipements réseaux ainsi que les machines informatiques. Ce protocole est donc utilisé par les administrateurs réseaux pour détecter à distance les problèmes qui surviennent sur leur réseau.

Chaque machine, que ce soit sous Windows ou sous Linux possèdent de nombreuses informations capitales pour l'administrateur réseaux. On retrouve des informations comme la quantité de RAM utilisé, l'utilisation du CPU, l'espace disque et encore bien d'autre indicateurs. SNMP va permettre de remonter ces informations à l'administrateur de façon centralisé pour pouvoir réagir au plus vite aux pannes éventuelles.

III.2.Fonctionnement

III.2.1 Les agents

Sur une machine à superviser, pour que SNMP envoie les informations que l'on souhaite il faut qu'un agent soit installé sur celle-ci. Cet agent écoute sur le port 161 et attend que le serveur lui envoie des requêtes pour lui répondre.

L'agent pourra aussi envoyer des alertes lui même si l'administrateur l'a configuré. Par exemple pour surveiller l'occupation CPU l'administrateur définira une valeur critique pour laquelle une alerte doit lui être émise.

Pour finir l'agent pourra aussi agir sur l'environnement local. C'est pourquoi ce protocole est critique car il peut servir à d'autres personnes mal intentionnées pour prendre le contrôle à distance de certains équipements sur le réseau.

III.2.3 La MIB

- Présentation

Pour que SNMP fonctionne, il est nécessaire qu'un protocole d'échange soit définit. Il y a aussi une standardisation des informations que ce protocole peut transporter. C'est un protocole Internet, il doit être utilisable sur des plates-formes hétérogènes (matériel comme système d'exploitation).

C'est pour cette raison que l'on parlera de MIB (Management Information Base).En effet, la MIB est une base de données des informations de gestion maintenue par l'agent. C'est cette base à laquelle on va demander les informations.

- Structure de la MIB

La structure de la MIB est hiérarchique : les informations sont regroupées en arbre. Chaque information a un OID (Object identifier), une suite de chiffres séparés par des points, qui l'identifie de façon unique et un nom, indiqué dans le document qui décrit la MIB.

Par exemple, 1.3.6.1.2.1.2.2.1.2 est l'OID ifDescr qui est la chaîne de caractères décrivant une interface réseau (comme eth0 sur Linux ou Ethernet0 sur un routeur Cisco).

Une des MIB les plus connues est MIB-II, décrite dans le RFC 1213, et qui est mise en œuvre dans quasiment tous les équipements TCP/IP. Elle compte dix groupes : « système », «interfaces », « at », « IP », « ICMP », « TCP », « UDP », « EGP », « transmission » et « SNMP ».

III.2.4 Les commandes SNMP

Il existe 4 types de requêtes SNMP :

- get-request: Le Manager SNMP demande une information à un agent SNMP
- get-next-request: Le Manager SNMP demande l'information suivante à l'agent SNMP
- set-request: Le Manager SNMP met à jour une information sur un agent SNMP
- trap: L'agent SNMP envoie une alerte au Manager

Les alertes sont transmises lorsqu'un événement non attendu se produit sur l'agent. Ce dernier informe le manager via une « trap ». Plusieurs types d'alertes sont alors possibles : ColdStart, WarmStart, LinkDown, LinkUp, AuthentificationFailure.

Pour chaque envoi de message, une réponse est retournée à l'exception de la commande «trap ».

Les réponses sont du type suivant :

- get-response: L'information a bien été transmise.
- NoSuchObject: Aucune variable n'a été trouvée.
- NoAccess: Les droits d'accès ne sont pas bons.
- NoWritable: La variable ne peut être écrite.

III.2.5. Echange de message

Voici un schéma récapitulant les échanges pouvant être effectués entre un agent et le manager :

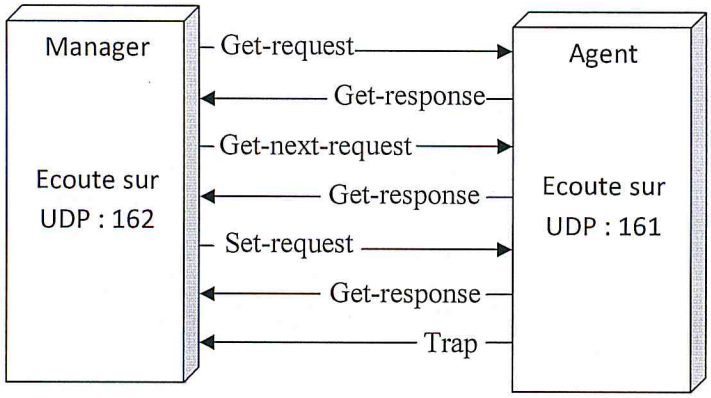


Fig.5 Exemple d'échange SNMP

Le protocole SNMP est principalement utilisé avec UDP/IP. (Il peut aussi utiliser TCP). L'utilisation d'UDP permet un échange de message plus rapide que l'utilisation de TCP. L'inconvénient est qu'il est possible de perdre des trames lors de l'échange de messages (mode non connecté). Les ports UDP sont donc le 162 pour le manager et le 161 pour les agents.

III.3. Avantages et inconvénients

Nous l'avons vu, le protocole SNMP a de nombreux avantages en tant qu'outil de gestion réseau :

- Accès centralisé: la gestion réseau s'effectue depuis une machine centrale sans soucis, et c'est même préférable pour la sécurité.
- Sécurité: la sécurité s'est accrue au cours des différentes versions, jusqu'à respecter la plupart des contraintes imposées.
- Fiabilité: le protocole utilisé permet de s'assurer que les requêtes sont bien arrivées à destination et qu'elles ont été correctement interprétées.
- Evolutivité: l'utilisation d'une arborescence pour la gestion des variables permet d'avoir une évolution continuelle des capacités fonctionnelles accessibles via ce protocole.
- Gestion de la diversité: l'utilisation d'une interface standard à tous les matériels permet de contrôler de la même manière tous les équipements réseaux, ce qui a des avantages indéniables lorsque l'on dispose d'un parc informatique très diversifié.

Toutefois, certains reproches peuvent être faits à SNMP : l'interface standard de communication est très pauvre et ne fournit qu'un nombre très limité d'informations : état des

interfaces réseaux, nombre d'octets transmis, etc.... mais tous les constructeurs ont décidé d'exploiter leurs spécificités directement dans leur MIB propre plutôt que d'essayer d'uniformiser au maximum et de faire évoluer la MIB standard. Ainsi, même si certaines informations peuvent être obtenues identiquement sur des matériels distincts, il sera parfois nécessaire de rechercher dans la MIB du constructeur pour obtenir des informations plus pointues. [3]

IV. Les logiciels de supervision

IV.1.Des logiciels libres

IV.1.1 MRTG

MRTG est un outil pour surveiller la charge de la circulation des données qui transitent sur un réseau, un sous-réseau ou sur certaines machines via SNMP. Il produit des pages HTML contenant des images qui fournissent une représentation visuelle du trafic désiré. MRTG est basé sur les langages Perl et C, il fonctionne sous UNIX et Windows NT. Son succès a été très important et son successeur RRDTool qui est écrit par le même auteur est maintenant utilisé dans de nombreux logiciel de monitoring.

IV.1.2. CACTI

Cacti est un logiciel de supervision qui est un front-end (interface graphique) de RRDTool. Il est basé sur un serveur web avec une base de données MySQL et PHP. RRDTool permet de stocker toutes les informations de supervision réseau et de générer des graphiques. MRTG est utilisé pour récupérer ces informations avec SNMP.

CACTI permet donc de représenter graphiquement divers statuts de périphériques réseau utilisant SNMP ou encore grâce à des scripts (Bash, PHP, Perl, VBs...) pour avoir par exemple l'espace disque restant ou encore la mémoire utilisée, la charge processeur ou le ping d'un élément actif.

IV.1.3 Nagios

Nagios est un logiciel qui permet de superviser un système d'information complet. C'est un logiciel libre, il est sous licence GPL. Les fonctionnalités de Nagios sont nombreuses.

La première particularité de Nagios est la modularité. En effet des plugins peuvent être ajoutés pour effectuer des taches spécifiques. De nombreux plugins sont déjà écrits par la communauté Nagios mais nous pouvons en écrire nous même pour des taches spécifiques.

Nagios va être couplé avec Oreon qui va permettre de faciliter l'administration mais aussi remonter les graphes et effectuer du reporting. Nagios intègre bien sur une notification par mail ou sms selon le jour et l'heure. Voici les avantages/inconvénients de Nagios :

Avantages :

- Surveillance des services réseaux (SMTP, POP3, HTTP, NNTP, PING, etc.).
- Surveillance des ressources des hôtes (charge processeur, utilisation des disques, etc.).
- Système simple de plugins permettant aux utilisateurs de développer facilement leurs propres vérifications de services.
- Notifications des contacts quand un hôte ou un service a un problème et est résolu (via email, pager, ou par méthode définie par l'utilisateur).
- Possibilité de définir des gestionnaires d'évènements qui s'exécutent pour des évènements sur des hôtes ou des services, pour une résolution des problèmes
- Interface web, pour voir l'état actuel du réseau, notification et historique des problèmes, fichiers log, etc.
- Plugins existant pour utiliser MRTG ou RRDTool

Inconvénients :

- Configuration compliquée qui oblige une très bonne connaissance de Nagios.
- Graphes pas assez clairs.
- Administration compliquée.

IV.1.4. Oreon

Oreon consiste à inclure dans une solution complète l'ensemble des services de Nagios existants, ainsi que des modules d'installation et de configuration du serveur Nagios. Oreon est en perpétuelle évolution grâce au monde open source très actif autour de ce projet, ce qui permet une aide en cas de problème à travers les différents forums et des évolutions logicielles permettant une efficacité accrue et la correction de bug logicielle rapide.

Avantages :

- Une installation complète et automatique des packages nécessaires à l'utilisation de NAGIOS.
- Facilite la configuration de Nagios.
- Une découverte automatique du réseau et une configuration des ressources découvertes (serveurs, équipements réseaux...) au niveau du serveur de supervision. L'utilisateur

n'aurait plus qu'à sélectionner la ressource à superviser et lui indiquer quel type d'alerte qu'il souhaite remonter.

- Graphe le résultat des alertes, système de reporting.

Inconvénients:

- Requiert plus de ressources matérielles.
-

IV.2. Des logiciels propriétaires

2.1 IBM Tivoli Netview

Ce logiciel est né du rachat de l'entreprise Tivoli par IBM. C'est un des logiciels commercial le plus utilisée. Il s'agit d'une suite de logiciels comprenant notamment Tivoli Monitoring essentiellement dédié à la supervision de machines ou d'applications.

L'architecture repose sur le protocole SNMP. Des agents sont en places sur chaque matériel et une application centrale permet d'effectuer divers opérations :

- Définir les différentes règles de supervision.
- Stocker les informations et les présenter sous la forme de pages web.
- Générer différents graphiques sur l'état du réseau.

Chaque machine qui est supervisée doit posséder un environnement d'exécution JAVA. Tivoli Monitoring s'occupe de récupérer les informations sur les machines : occupation processeur, système de fichier.

Afin de compléter les fonctions de cet outil, il est possible de le compléter avec une suite logicielle : Tivoli Business Systems Manager qui permet alors de disposer d'un ensemble de gestion de système d'information relativement complet :

- Découverte des réseaux TCP/IP
- Affichage des topologies réseaux
- Gestion des différents événements
- Affichage de la santé et de l'état du réseau
- Détection et prévention de problèmes

Il est également possible d'analyser des différents flux échangés dans un réseau.

Les principaux avantages de cette solution est que c'est sans aucun doute une des plus répandue sur le marché. Elle est s'adapte facilement à notre besoin et est relativement complètes.

Un des inconvénients est qu'il faut posséder une grande partie de la gamme afin de pouvoir superviser le mieux possible un réseau.

2.2 HP OpenView

HP OpenView est aussi un des logiciels majeur de la supervision à l'heure actuelle. Il permet le management d'équipements réseau. Une interface graphique permet un affichage de l'état courant des équipements. Un système d'alarme permet de synchroniser le tout. Il est basé sur SNMP pour dialoguer avec les différentes machines.

OpenView intègre un système d'alarme. En effet des requêtes SNMP sont régulièrement effectuées vers les agents. Si un état change ou une machine devient injoignable, une alarme est directement déclenchée et une action peut-être déclenchée. (Lancement d'un programme, envoie d'un mail…)

Ses principaux atouts sont les suivants :

- Une vue globale du système d'information
- Une vision des différents incidents
- Un contrôle homogène des différents matériels

V. Avenir de la supervision

V.1.Avenir de SNMP

SNMP est un protocole plein d'avenir : il se développe de plus en plus ces dernières années, parallèlement à l'essor des réseaux. La seule crainte que l'on puisse avoir est que les constructeurs, plutôt que d'adopter et de continuer à faire évoluer ce protocole devenu standard, continuent d'exploiter leurs propres protocoles, détruisant un espoir d'uniformisation de la gestion réseau.

En soi, le protocole SNMP a beaucoup d'avantages indéniables que nous avons pu mettre en avant, et les implémentations de celui-ci sont de plus en plus solides et fournissent des bases de plus en plus intéressantes aux développeurs et aux intégrateurs de systèmes.

V.2.Autres standards

Plusieurs autres solutions de supervision semblent se tourner vers Internet. En effet, plusieurs standards existent déjà :

- WEBMEN qui spécifie un modèle de données pour l'administration. De nombreuses organisations supportent à l'heure actuelle ce standard tel que HP, Microsoft…
- Le protocole d'administration HMMP. (Hypermedia Management Protocol), une sorte de SNMP sur Internet. Il s'agit d'un protocole de communication au dessus de http qui achemine les requêtes HMOM (commandes associées au protocole) jusqu'à un serveur Web. Il supporte également les requêtes fondées sur des objets comme les contrôles ActiveX, Com/Dcom, Corba, des plugins...

- JMAPI (Java Management Application Programming Interface), une interface de programmation qui permet d'écrire des agents Java et des applications d'administration. Il s'agit d'un ensemble d'objets permettant de créer très facilement des applications d'administration de réseaux et de services. Il contient une interface homme machine d'administration des ressources, des interfaces de notification d'événements, de demande d'actions sur une ou plusieurs ressources, des interfaces de gestion des données en base de données, des interfaces SNMP.
- WS-Management (Web Services Management) est une spécification qui permet de simplifier l'administration des services web. Elle décrit notamment la façon de programmer un firmware ou un logiciel afin de permettre à un administrateur système d'éteindre ou d'allumer à distance un matériel ou un logiciel et de diagnostiquer un dysfonctionnement, quel que soit l'endroit où il se trouve. Ce protocole pourrait aussi être utilisé pour administrer des modems ADSL, des télévisions, des lecteurs de DVD... Ce protocole devrait être intégré dans les prochaines versions de Microsoft Windows Server.

VI. Conclusion

La supervision est devenue indispensable dans tout système d'information. Elle est à la base du bon fonctionnement d'une architecture réseau et permet de réagir rapidement en cas de problèmes ou pannes. Elle se base à l'heure actuelle principalement sur le protocole SNMP qui depuis de nombreuses années a quand même du mal à évoluer. En effet, de nombreux logiciels sont encore basés sur la version 1 du protocole qui commence un peu à vieillir et qui n'est pas du tout sécurisé. En effet la version 2, apportant notamment la sécurité n'a été qu'une phase de transition vers la v3 qui est encore très peu utilisée.

Les logiciels de monitoring sont très nombreux qu'ils soient du monde du libre ou propriétaires et supportent les principales plateformes des systèmes d'information. La plupart sont encore basés sur le protocole SNMP. On peut alors se demander si les nouveaux standards qui sont encore au statut de développement seront utilisés dans un avenir proche et amené à le remplacer?

Chapitre III

Conception

I. INTRODUCTION

En génie logiciel la conception constitue une phrase fondamentale dans le cycle de vie d'un logiciel, la réussite de ce dernier dépend beaucoup dans cette étape. Dans notre application on va se baser sur deux conceptions, la conception architecturelle et la conception détaillée.

II. LA NOTATION U.M.L (UNIFIED MODELING LANGUAGE)

Langage de Modélisation Unifié, possède un formalisme qui est une fusion des notations de Booch, OMT, OOSE et d'autres notations. La méthodologie UML est conçue pour être lisible sur des supports très variés. Les concepteurs de la notation ont recherché avant tout la simplicité; UML est intuitive, homogène et cohérente. Les symboles embrouillés, redondants ou superflus ont été éliminés en faveur d'un meilleur rendu visuel.

La méthodologie UML se concentre sur la description des artefacts du développement de logiciel, plutôt que sur la formalisation du processus de développement lui-même, elle peut ainsi être utilisée pour décrire les éléments logiciels, obtenus par l'application de différents processus de développement.UML ne recherche pas la spécification à outrance, il n'y a pas une représentation graphique pour tous les concepts imaginables ; en cas de besoins particuliers des précisions peuvent être apportées au moyen de mécanismes d'extension et de commentaires textuels de l'utilisateur. Les diagrammes d'UML peuvent montrer tout où partie des caractéristiques des éléments de modélisation, selon le niveau de détail utile dans le contexte d'un diagramme donné. Voici, la liste des différents diagrammes.

- **Les diagrammes d'activités** qui représentent le comportement d'une opération en termes d'actions ;
- **Les diagrammes de cas d'utilisation** qui représentent les fonctions du système du point de vue de l'utilisateur ;
- **Les diagrammes de classes** qui représentent la structure statique en termes de classes et de relations ;
- **Les diagrammes de collaboration** qui sont une représentation spatiale des objets, des liens et des interactions ;
- **Les diagrammes de composants** qui représentent les composants physiques d'une application ;
- **Les diagrammes de déploiement** qui représentent le déploiement des composants sur les dispositifs matériels ;
- **Les diagrammes d'états-transitions** qui représentent le comportement d'une classe en termes d'états ;
- **Les diagrammes d'objets** qui représentent les objets et leurs relations et correspondent aux diagrammes de collaboration simplifiés, sans représentation des envois de message ;
- **Les diagrammes de séquence** qui sont une représentation temporelle des objets et de leurs interactions. [4]

III. ANALYSE DES BESOINS

Un réseau est le résultat de l'interconnexion de plusieurs machines entre elles afin que les utilisateurs et les applications qui utilisent ces dernières puissent partager des ressources et échanger des informations, Pour garantir cette fonctionnalité, on doit concevoir un système permettant de contrôler les ressources partagées sur notre réseau à tout moment, ce système doit répondre aux besoins fonctionnels qui sont exprimés par des administrateurs de réseau ou des utilisateurs simples comme suit :

- Connaître toutes les machines qui sont connectées au réseau à un moment donné ;
- Lister les ressources partagées sur le réseau par machine ;
- Surveiller une ressource partagée.

Pour cela, nous travaillons sur un système de surveillance qui contrôle l'accès aux ressources partagées sur un réseau local, ce système est composé d'un scanner IP, qui permet de recenser toutes les machines accessibles, et un observateur des ressources partagées qui permet de récupérer des informations concernant le partage à un moment donné ainsi que les accès à ce partage. Comme complément, on a ajouté un outil permettant la récupération d'autres informations, qu'on a jugé d'importance pour un administrateur (utilisateurs, groupes locaux, …etc.).

IV. ARCHITECTURE

IV.1 Architecture Logicielle

Les objets de domaine se regroupent en quatre principaux paquetages :

- Un scanner IP.
- Un Observateur des ressources partagées.
- Un Observateur d'hôte.
- Une base de données pour le stockage des informations récupérées.

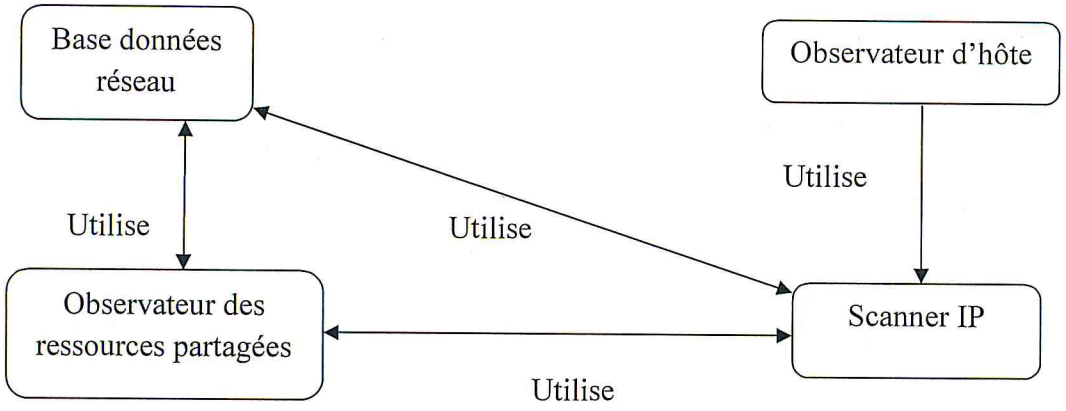


Fig.6: Paquetages de domaine « outil de surveillance des ressources partagées »

IV.2 Architecture matérielle

Les différents paquetages seront déployés comme suit :

Tous les paquetages de l'application seront installés sur le même PC connecté à un réseau local, ce PC peut appartenir à un groupe de travail ou un domaine.

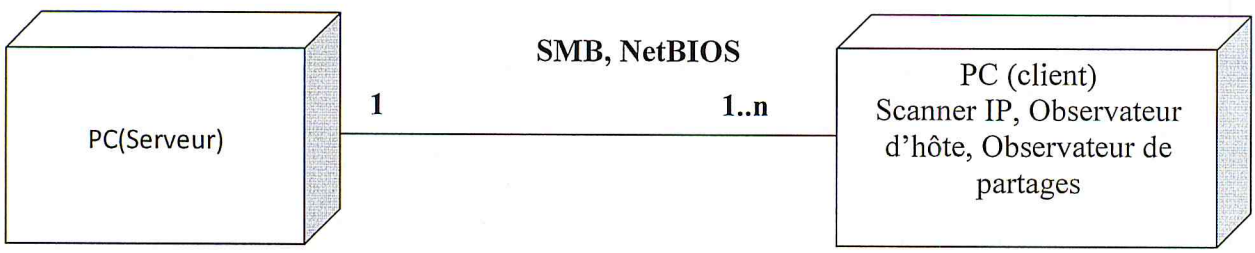


Fig.7: Diagramme de déploiement de domaine « outil de surveillance des ressources partagées »

V. LE SCANNER IP

V.1. Définition et fonctionnement :

Le scanner IP est une recherche de tous les serveurs accessibles dans un réseau local, alors, pour retourner la liste des ordinateurs connectés à notre réseau nous avons utilisé une méthode java très simple `namePC =InetAddress.getByName(IP).getHostName().toString()` a pour entrée toutes les adresses IP de la plage de scan de 1 à 254, elle retourne une liste contient des noms des ordinateurs et des adresses IP, les noms signifiés que ces ordinateurs sont accessibles par contre s'il retourne seulement des adresses IP alors ces ordinateurs ces sont pas accessibles, à partir de ce liste on prend seulement les noms des ordinateurs par la contrainte suivants : `if ( !namePC.startsWith( ip.toString()))` alors remplir le panneau de l'affichage de résultat par la fonction addPoste().

V.2. Détermination des cas d'utilisation

L'analyse débute par la recherche des acteurs du système. Un acteur représente un rôle joué par une personne, c'est un utilisateur qui utilise et communique avec le système.

Comment les rechercher? Ou comment faire l'Identification des acteurs.

Pour cela, on s'est posé les questions suivantes :

Qui utilise le système?

Qui installe le système?

Qui démarre le système?

Qui maintient le système?

Qui ferme le système?

Qui a besoin d'informations venant du système?

La réponse à toutes ces questions étant : un administrateur ou un simple utilisateur.

A partir de cette réponse, l'acteur du scanner IP est défini comme suit :

- Utilisateur : c'est une personne ou acteur utilisant le scanner IP. Il peut être un administrateur ou un simple utilisateur.

Après avoir défini les acteurs interagissant avec le scanner IP, on détermine ses cas d'utilisation. Il s'agit de montrer les différentes possibilités d'utilisation du système, et le comportement du système en réponse à une interaction d'un acteur.

Comment les rechercher? Ou comment faire l'Identification des cas d'utilisation.

On s'est posé les questions suivantes :

Quelles sont les fonctions demandées par l'utilisateur du système?

Réponse : l'utilisateur du système peut faire:

1. Modification de la plage d'adresses IP.
2. Tri de la liste de scan.

3. Effacer la liste de scan.

Le système mémorise t-il de l'information?

Réponse : oui

Quel acteur créera, lira mettra à jour l'information ?

Réponse : l'hôte créera ou mettra à jour l'information, l'utilisateur lira l'information.

A partir de ces réponses, Les cas d'utilisation énumérés sont :

Acteur	**Cas d'utilisation**
Utilisateur	• Modifier la plage d'adresses IP • Trier la liste de scan trouver ; • Effacer la liste ; • Enregistrer le résultat.

Tab.2: Cas d'utilisation du système Scanner IP

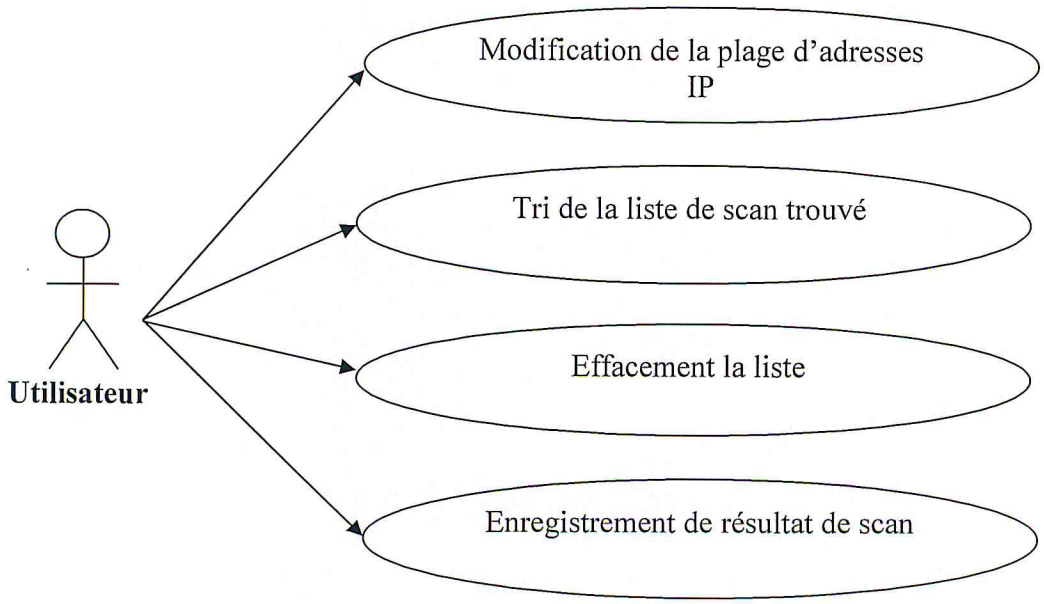


Fig.8 : Diagramme des cas d'utilisation du scanner IP

V.3. Description des cas d'utilisation

V.3.1. Modification de la plage d'adresses IP

La plage d'adresse IP se limite par la partie réseau de l'adresse IP, dans ce cas d'utilisation s'exécutent les actions suivantes :

- L'utilisateur démarre l'application ;
- Le système lui répond par une interface de saisie ;
- L'utilisateur modifie la plage de scan ;
- Le système contrôle et valide le choix.

La figue illustre bien ce cas d'utilisation.

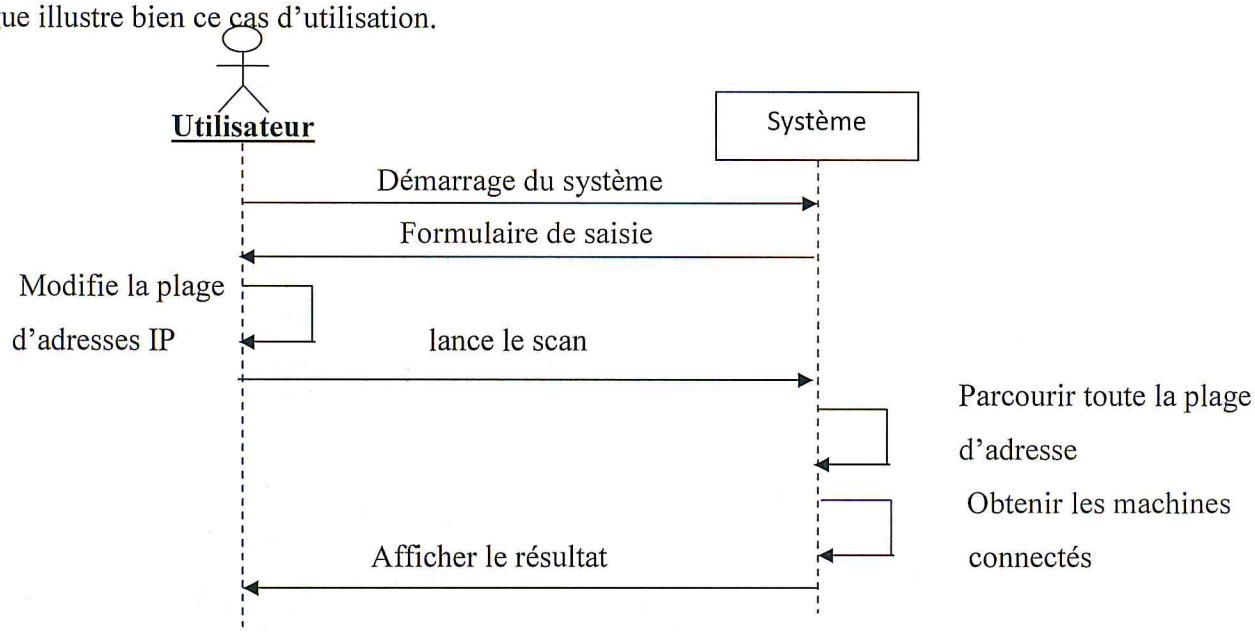


Fig.9. diagramme de séquence Modification de la plage d'adresses IP

V.3.2. Tri du résultat de scan

Ce cas d'utilisation comporte les actions suivantes :

- L'utilisateur démarre le scan ;
- Le système lui répond par une liste des serveurs accessibles ;
- L'utilisateur trié la liste par ordre alphabétique ;
- Le système contrôle et valide le choix.

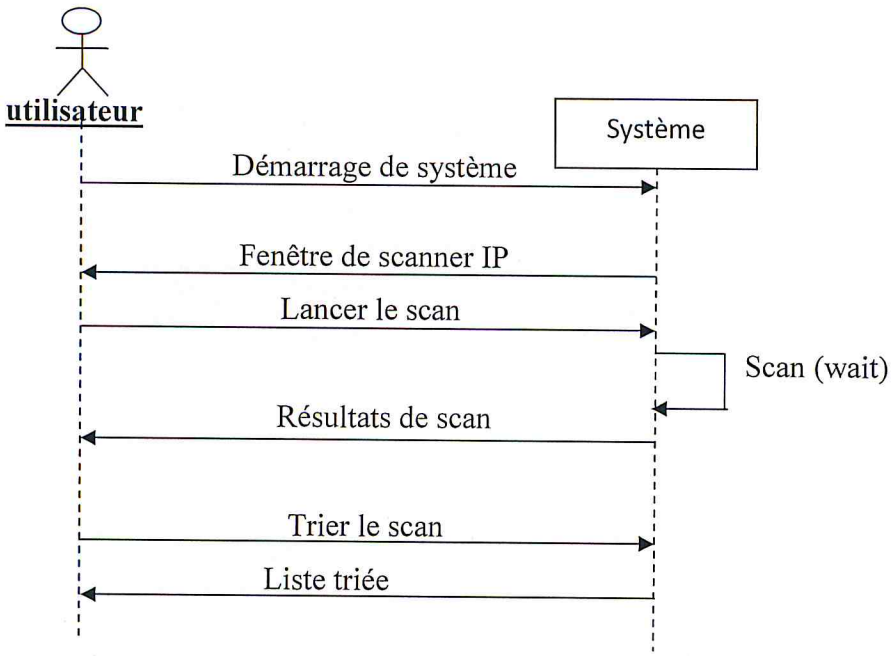


Fig.10. diagramme de séquence de tri du résultat de scan

V.3.3. Enregistrement de résultat de scan

Ce cas d'utilisation comporte les actions suivantes :

- L'utilisateur lance le scan ;
- Le système lui répond par une liste des serveurs accessibles ;
- Le système enregistré le résultat dans la base de données ;

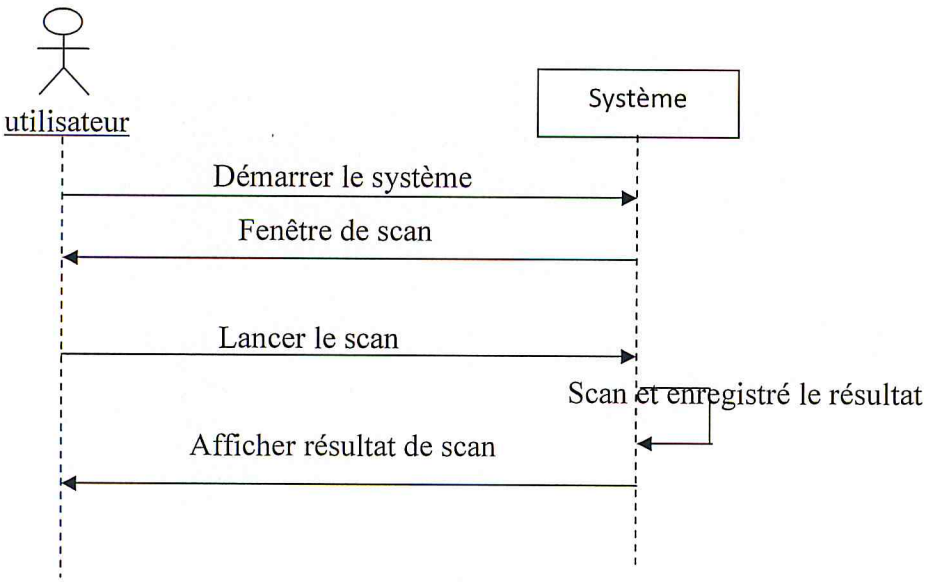


Fig.11. diagramme de séquence d'enregistrement de résultat de scan

V.3.4. Effacement de la liste de scan

Ce cas d'utilisation comporte les actions suivantes :

- L'utilisateur lance l'opération de scan;
- Le système lui répond par une liste des serveurs accessibles ;
- L'utilisateur effacer la liste ;
- Le système contrôle et valide le choix.

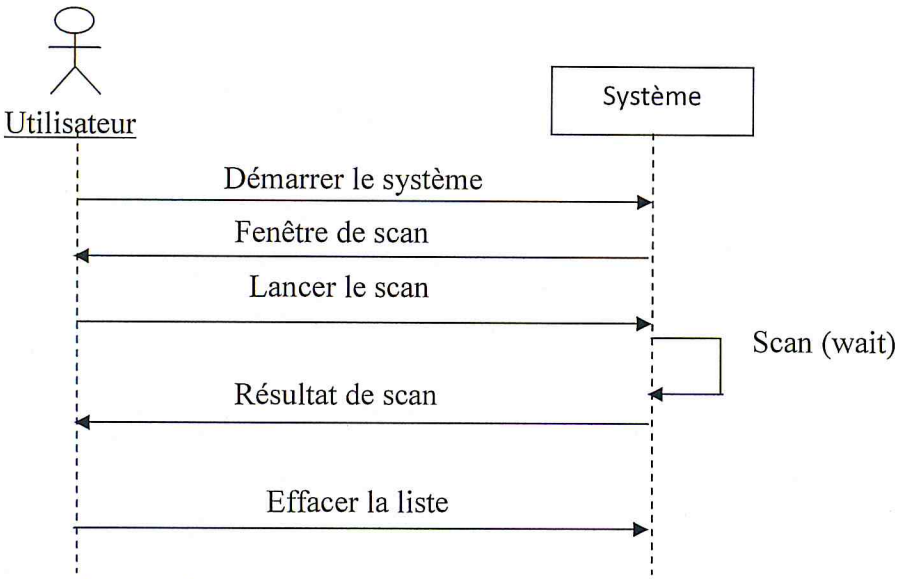


Fig.12. diagramme de séquence d'effacement de la liste de scan

V.4.1. Modification de la plage d'adresses IP

Ce cas d'utilisation se réalise par collaboration des deux objets : « Scanner IP », et un objet d'interface «ListeDestination ».

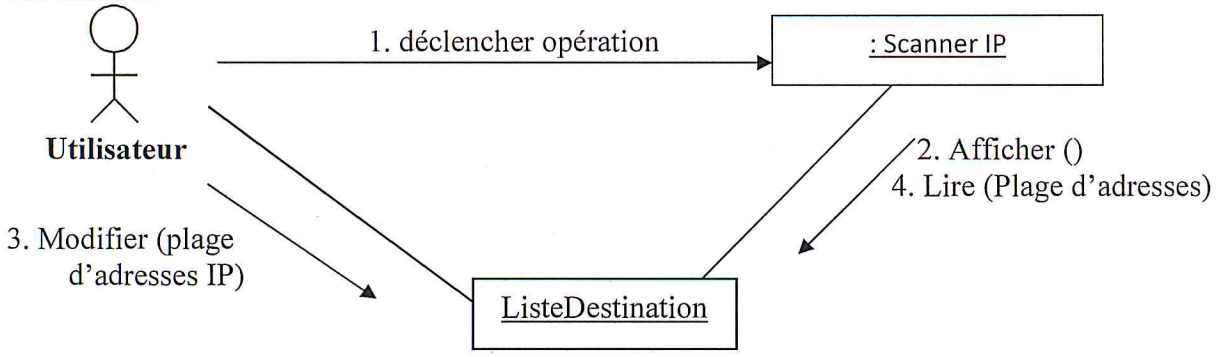


Fig.13 : Modification de la plage d'adresses IP par collaboration entre objets

V.5. Diagramme de classes de scanner IP

Un diagramme de classes du système Scanner IP est représenté comme suite :

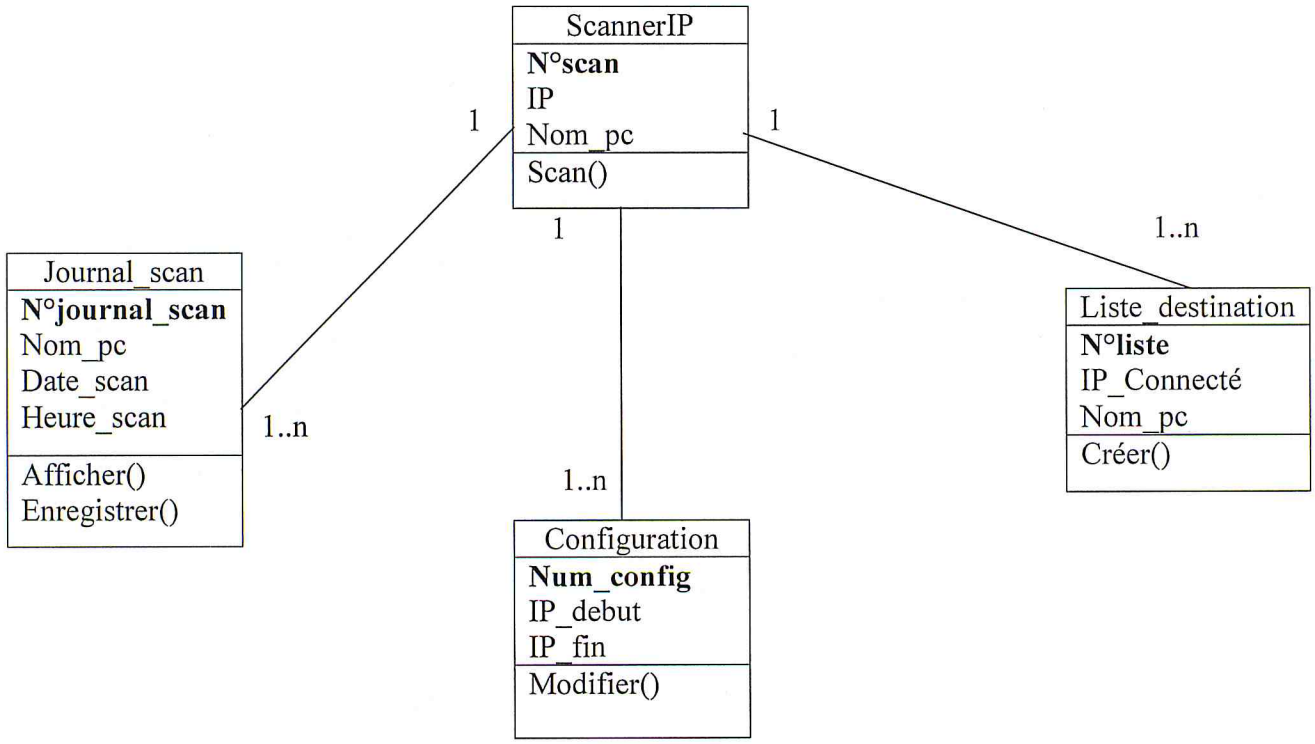


Fig.14 : Diagramme de classes de système Scanner IP

VI. L'OBSERVATEUR DES PARTAGES PAR HOTE

VI.1. Définition et fonctionnement

Le partage de fichiers consiste à rendre disponible à travers le réseau le contenu d'un ou plusieurs répertoires. Tous les systèmes Windows possèdent en standard des mécanismes permettant de mettre facilement en partage le contenu d'un répertoire. Néanmoins le partage de fichiers peut poser des problèmes de sécurité, car, par définition, il donne accès aux autres utilisateurs au contenu d'une partie du disque dur. (Comment ça marche).

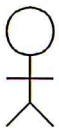
Cet outil offre à l'utilisateur la possibilité de surveiller la ressource partagée dans une machine distante, l'utilisateur doit aussi s'authentifier en tant qu'administrateur sur le serveur sélectionné. Pour afficher les partages d'une machine distante nous avons utilisé le Protocol SMB (Server message block) qui permet de récupérer toutes les partages d'un réseau ces adresses, ces utilisateurs etc.

D'autre part, l'observateur des partages par hôte permet aussi de consulté le contenu (répertoires, fichiers) de chaque partage, supprimé ce contenu, caché, ou changé le type d'accès d'un fichier.

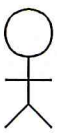
VI.1.2. Détermination des cas d'utilisation

Dans ce système participe les acteurs suivants :

- **Administrateur** : c'est une personne ou acteur utilisant l'observateur des ressources partagées.
- **Serveur** : peut être le réseau local au sens large, comme il peut être le serveur, désirant récupérer ses informations.
- **Scanner IP** : c'est le sous système fournissant à l'observateur de partage la liste des différents serveurs accessibles.



Serveur



Administrateur

Scanner IP

Après analyse de domaine, il ressort que les catégories des besoins fonctionnels des acteurs se décomposent de la manière suivante :

Acteur	Cas d'utilisation et principaux scénarios
Administrateur	Sélection d'un serveur ; Demande de connexion au serveur ; Ajout d'un nouveau répertoire dans un partage ; Supprimer répertoire de partage ; Cacher un répertoire ; Changer le type d'accès de répertoire (lecture, écriture) Ajouter un nouveau partage.
Serveur	Validation d'authentification ; Vérification d'identité ; Communication.
Scanner IP	Création d'un groupe de serveurs accessibles.

Tab.3 cas d'utilisation d'observateur des partages par hôte

La figure montre le diagramme des cas d'utilisation du système Observateur des ressources partagées.

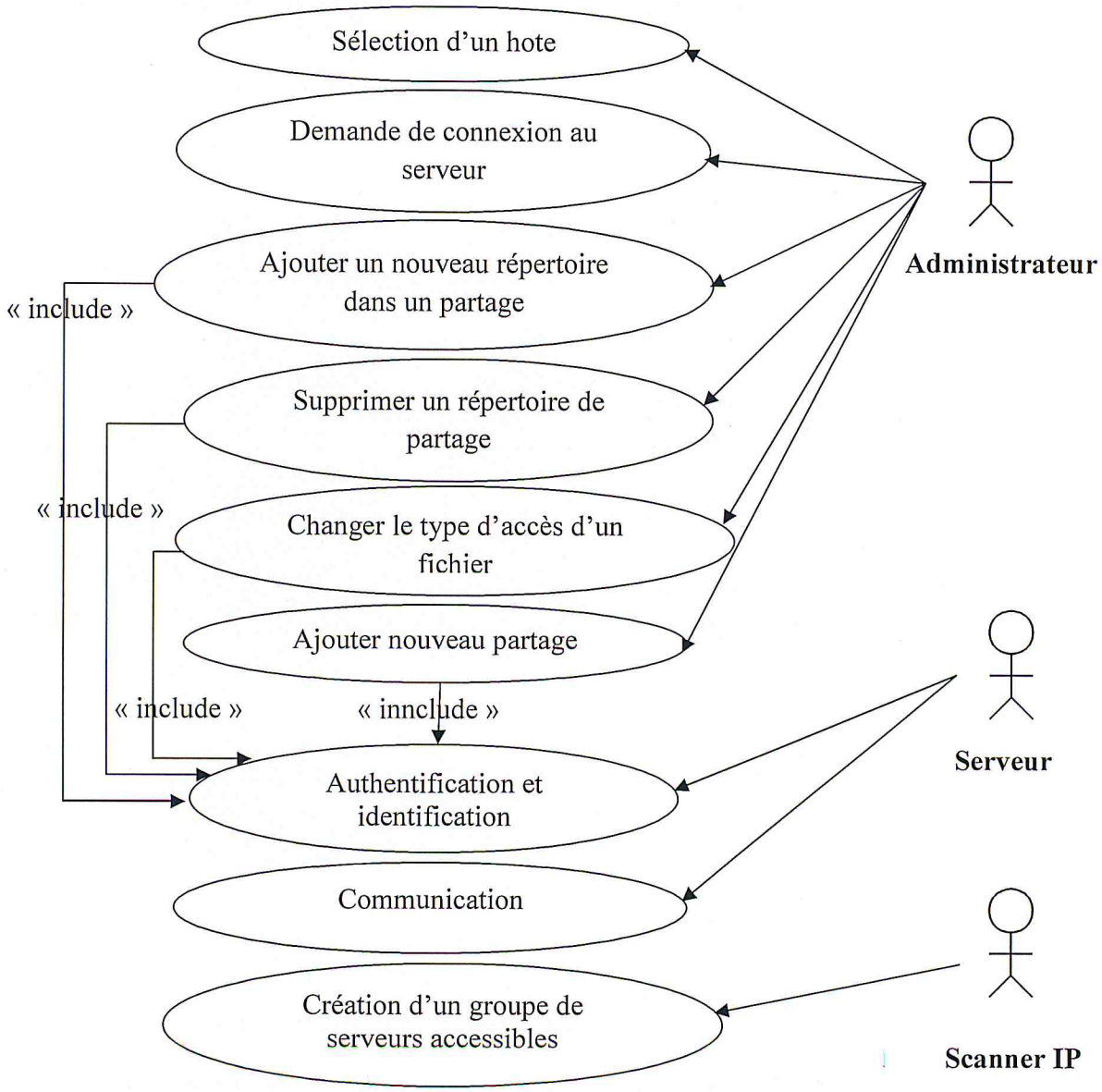


Fig. 15 : Diagramme des cas d'utilisations de l'observateur des ressources partagées

VI.3. Description des cas d'utilisations

VI.3.1 Création d'un groupe de serveurs accessibles

Ce cas d'utilisation permet de fournir une liste des serveurs, accessibles. Cette liste permet à l'administrateur de sélectionner le serveur désirant l'observer.

Les actions qui s'exécutent sont :

- Le scanner IP effectue une opération de scan ;
- Le scanner IP établit la liste des serveurs accessibles.
- Le Scanner IP enregistre la liste des serveurs ;
- L'observateur des partages exploite la liste.

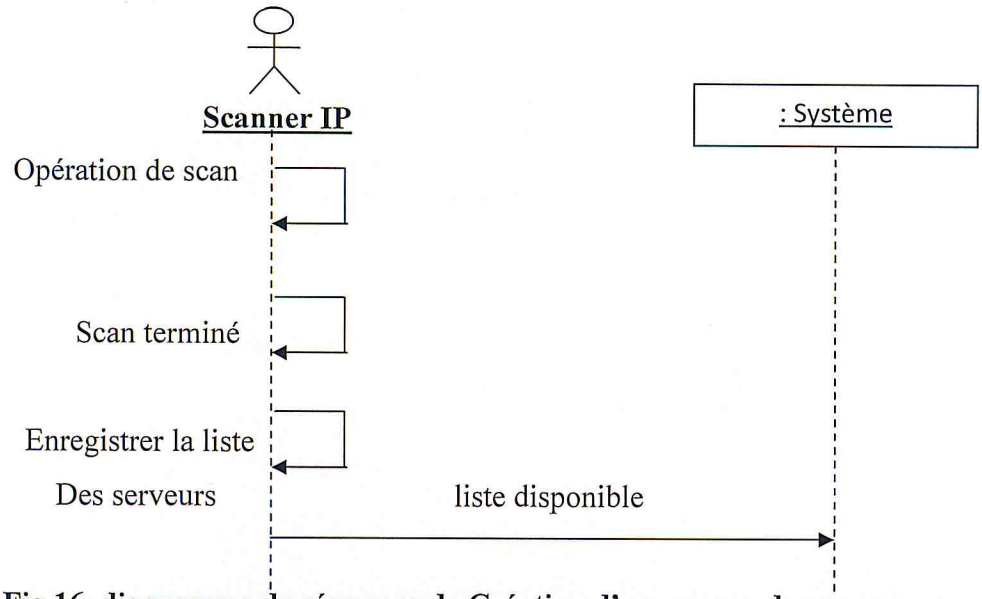


Fig.16. diagramme de séquence de Création d'un groupe de serveurs accessibles

VI.3.2 Sélection d'un serveur et demande de connexion

Ce cas d'utilisation permet à l'administrateur de sélectionner un serveur qui désire l'observer. Les actions qui s'exécutent sont :

- L'administrateur déclenche la fenêtre observateur d'hôte qui contient la sélection d'un serveur ;
- Le système lui répond par une interface contenant la liste des serveurs accessibles ;
- L'administrateur sélectionne un serveur ;
- Le système lui demande le nom utilisateur et le mot de passe, via une interface de saisie ;
- L'administrateur saisi, un nom utilisateur et un mot de passe ;
- Le système demande l'établissement de la connexion avec le serveur.
- Si la validation est terminée avec succès, le serveur crée une session pour cet utilisateur, sinon la connexion est refusée.

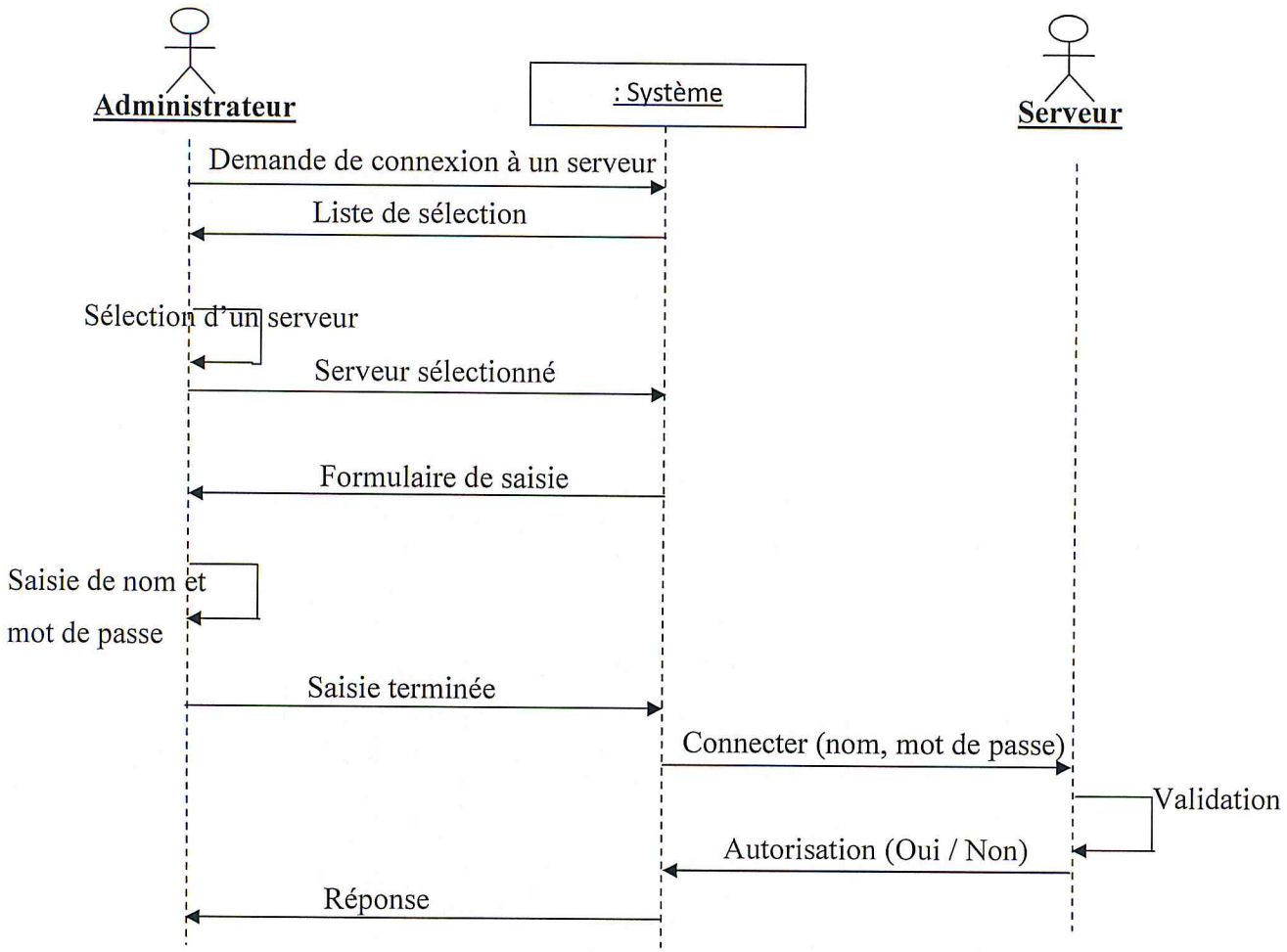


Fig.17. diagramme de séquence de Sélection d'un serveur et demande de connexion

VI.3.3 Scénario de suppression d'un répertoire de partage

Ce cas d'utilisation comporte les actions suivantes :

- L'administrateur déclenche l'opération de supprimé d'un répertoire ;
- le système lui répond par une liste de choix ;
- L'administrateur sélectionne un répertoire ;
- Le système supprime le répertoire.

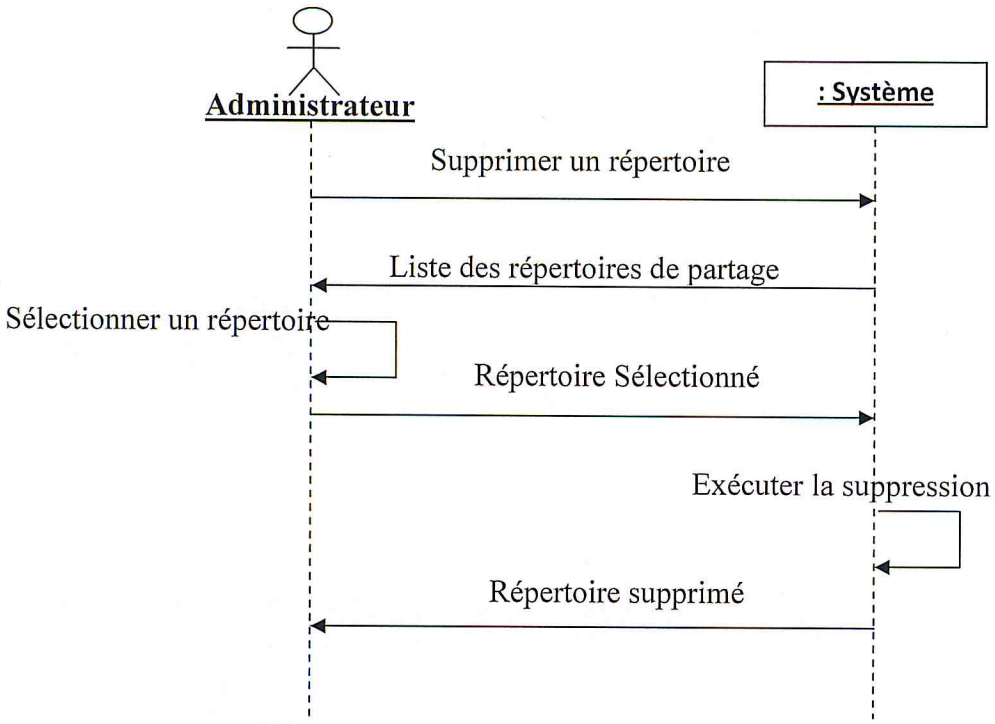


Fig.18. diagramme de séquence de suppression d'un répertoire de partage

VI.3.4 Scénario d'ajout d'un nouveau répertoire dans un partage

Ce cas d'utilisation comporte les actions suivantes :

- L'administrateur déclenche l'opération de l'ajout d'un nouveau répertoire ;
- le système lui répond par un formulaire ;
- L'administrateur sélectionne le serveur ;
- Le système lui répond par une liste des partages de ce serveur sélectionné;
- L'administrateur sélectionne le partage;
- L'administrateur ajoute le nom de répertoire et les autorisations d'accès ;
- Le système ajouté le répertoire dans le partage sélectionné.

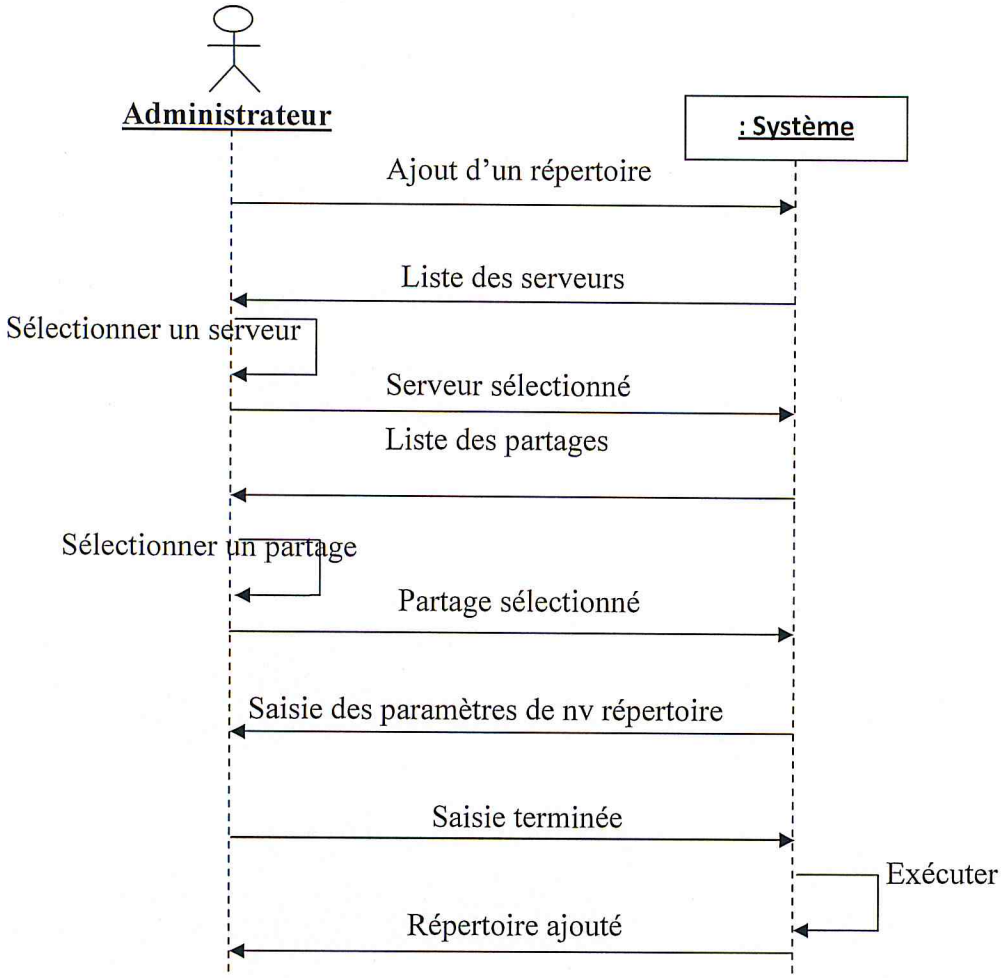


Fig.19. diagramme de séquence d'ajout d'un nouveau répertoire dans un partage

VI.3.5 Scénario de modifier le type d'accès d'un répertoire dans un partage

Ce cas d'utilisation comporte les actions suivantes :

- L'administrateur sélectionner un partage parmi la liste des partages ;
- le système lui répond par une des répertoires et des fichiers de ce partage;
- L'administrateur sélectionne le répertoire ou le fichier a modifié ;
- L'administrateur lacer l'opération de changement de type (lecture, écriture)
- Le système changé le type de répertoire ou de fichier.

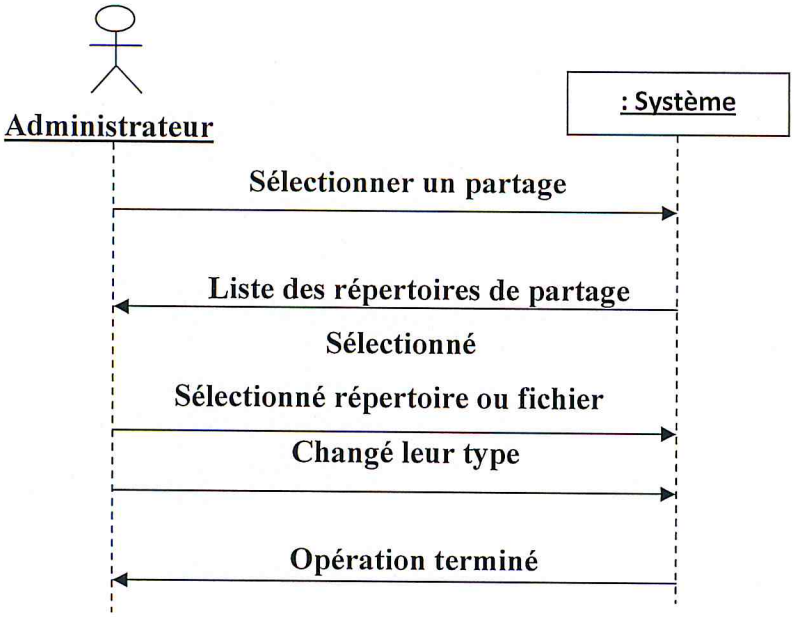


Fig.20. diagramme de séquence de modifier le type d'accès d'un répertoire dans un partage

VI.3.6. Scenario de cacher un répertoire ou un fichier dans un partage

Ce cas d'utilisation comporte les actions suivantes :

- L'administrateur sélectionner un partage parmi la liste des partages ;
- le système lui répond par une des répertoires et des fichiers de ce partage;
- L'administrateur sélectionne le répertoire ou le fichier a modifié ;
- L'administrateur lancé l'opération de cache ;
- Le système caché le répertoire ou le fichier sélectionné.

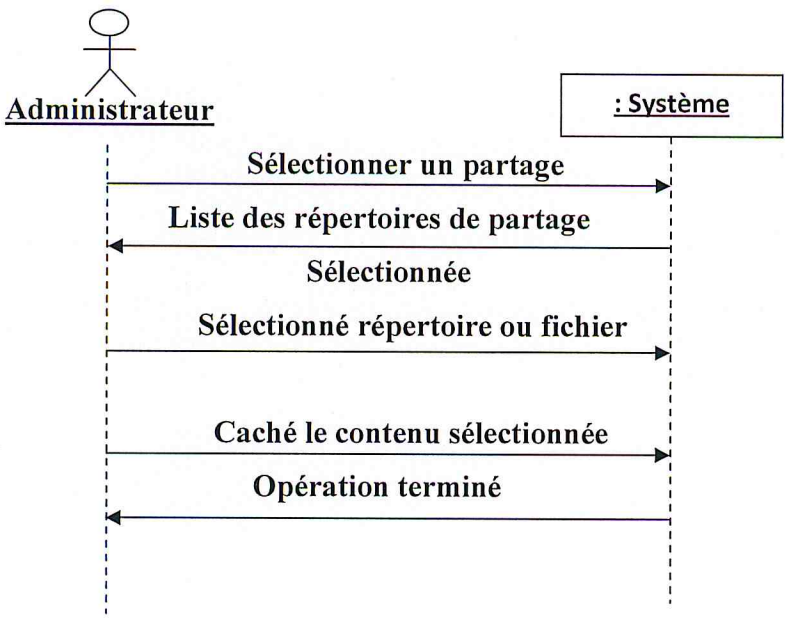


Fig.21. diagramme de cacher un répertoire ou un fichier dans un partage

VI.3.7. Scenario de création un nouveau dossier partagé

Ce cas d'utilisation comporte les actions suivantes :

- L'administrateur déclenche l'opération de l'ajout d'un nouveau partage ;
- Le système lui répond par assistant Création d'un dossier partagé (fenêtre Windows);
- L'administrateur spécifier un nom et une description pour le dossier partagé;
- L'administrateur spécifier les autorisations du dossier partagé puis terminer;
- Le système ajouté le nouveau dossier partagé.

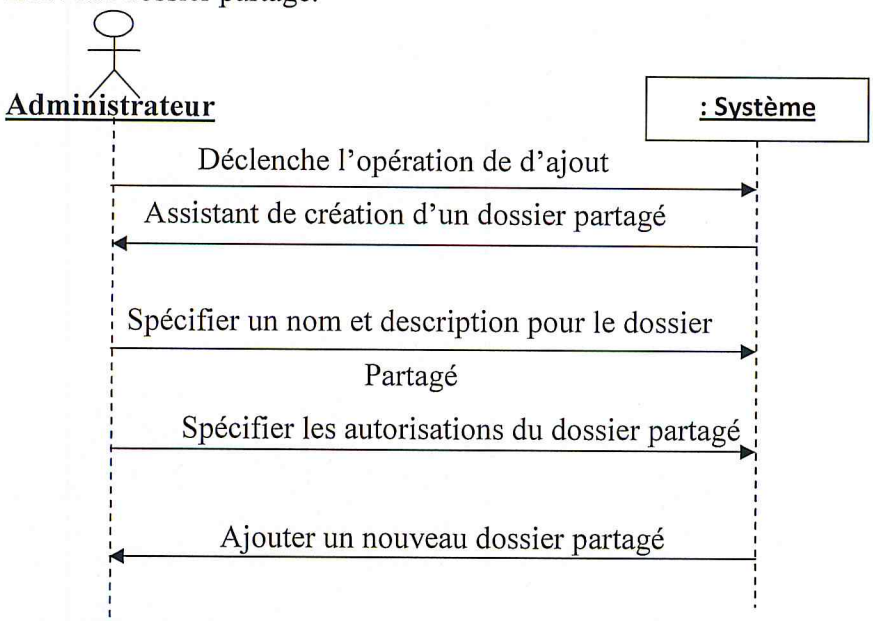


Fig.22. diagramme de séquence pour création un nouveau dossier partagé

VI.4. Description des collaborations

VI.4.1 Création de groupe de serveurs accessibles

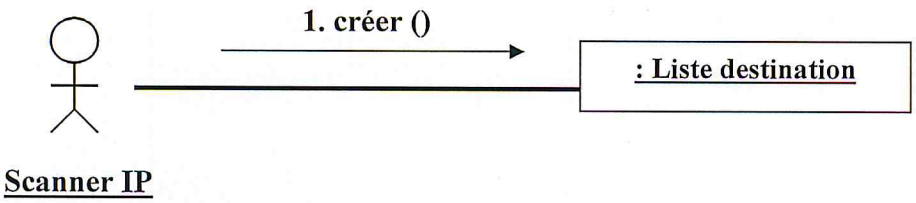


Fig.23. Création d'un groupe de serveurs accessibles par collaboration entre objets

VI.5. Diagramme de classes de l'observateur de partages par hôte

Un diagramme de classes du système Observateur de partage est présenté comme suit :

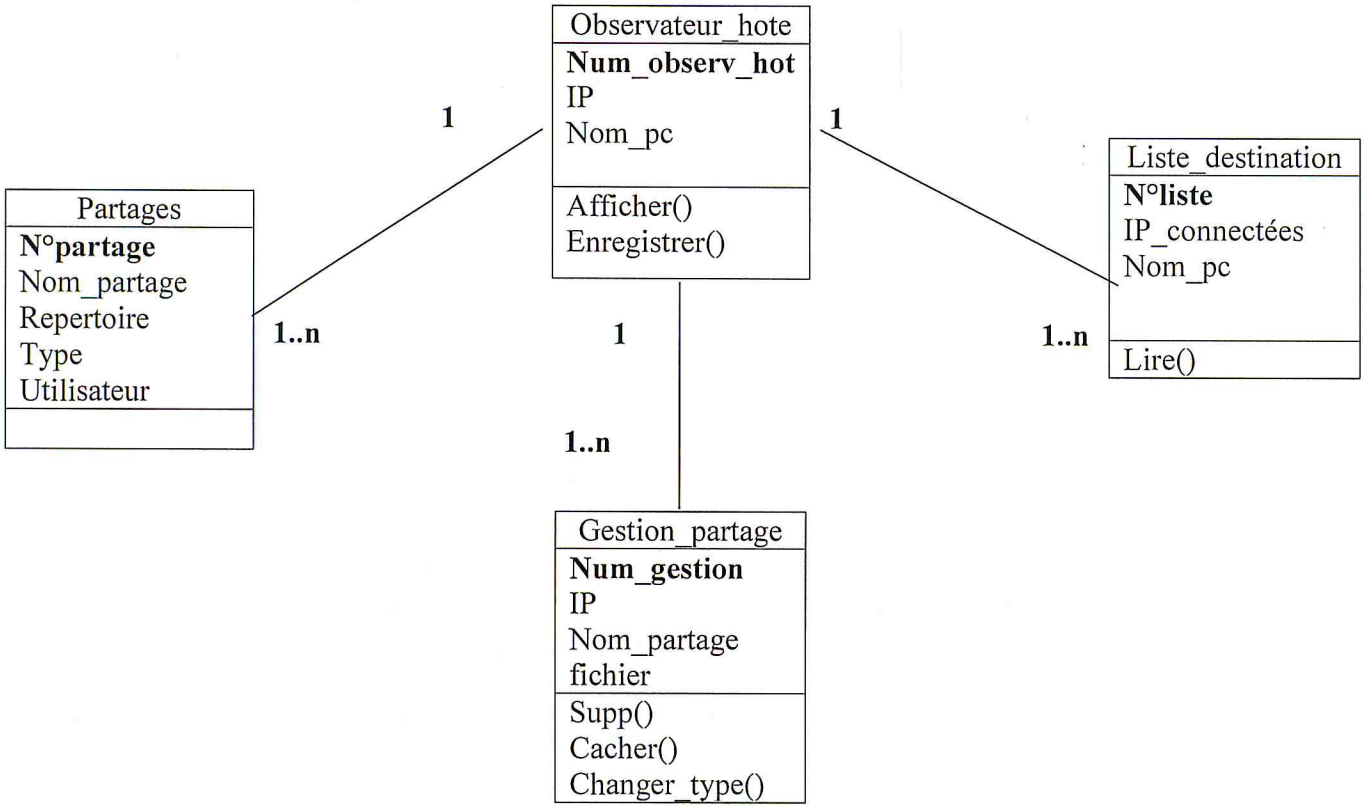


Fig.24.Diagramme de classes du système de l'observateur de partages par hôte

VII. L'OBSERVATEUR DES RESSOURCES PARTAGEES

VII.1. Définition et fonctionnement

Ce module permet de lister toutes les informations concernant les ressources partagées sur le réseau toujours par le protocole SMB, on donne la liste des machines accessible dans le réseau et il nous retourné une table contient toutes les partages de réseau par adresse et utilisateur.

VII.2. Détermination des cas d'utilisation

Dans ce système participe les acteurs suivants :

- Administrateur : c'est une personne ou acteur utilisant l'observateur d'hôte;
- Serveur : peut être le réseau local au sens large, comme il peut être le serveur, désirant récupérer ses informations ;
- Scanner IP c'est le sous système fournissant à l'observateur d'hôte la liste des serveurs qui sont accessible.

Après analyse de domaine, il ressort que les catégories des besoins fonctionnels des acteurs se décomposent de la manière suivante :

Acteur	Cas d'utilisation et principaux scénarios
Administrateur	Demande de connexion au serveur ; Lister les partages de tout le réseau ;
Serveur	Vérification d'identité ; Validation d'authentification ; Communication ;
Scanner IP	Création de groupe de serveurs accessibles.

Tab.4. Cas d'utilisation du système Observateur des ressources partagées

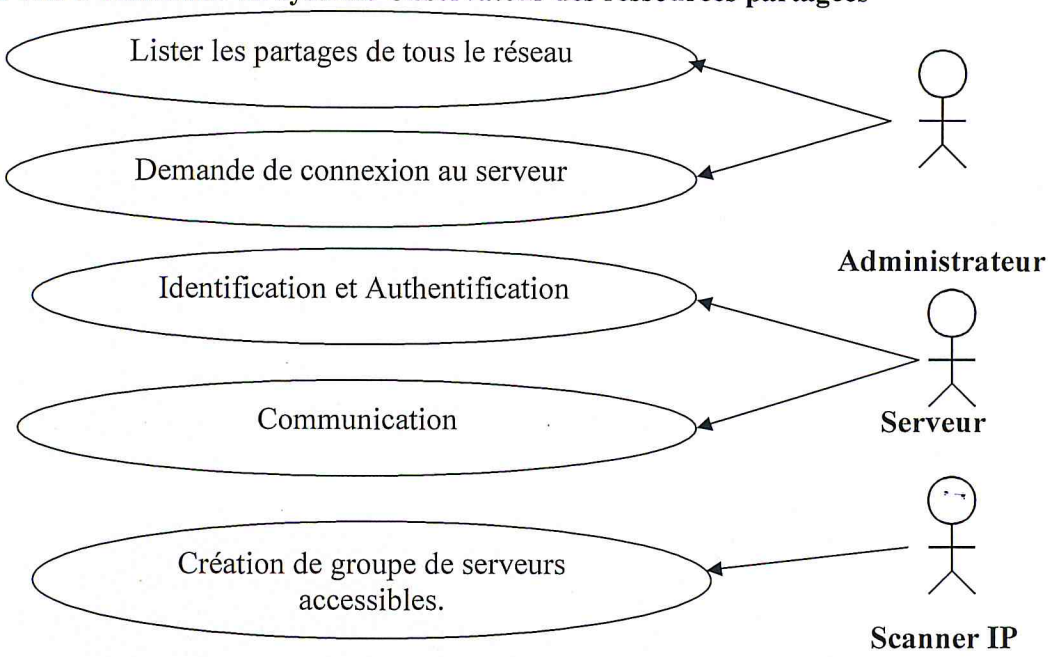


Fig.25. Diagramme des cas d'utilisation de l'observateur des ressources partagées

VII.3. Description des cas d'utilisation

VII.3.1 Création de groupe de serveurs accessibles

Ce cas d'utilisation permet de fournir une liste des serveurs accessibles. Cette liste permet à l'administrateur de sélectionner un serveur. Les actions qui s'exécutent sont :

- Le scanner IP effectue une opération de scan ;
- Le scanner IP fournit une liste des serveurs accessibles ;
- Le scanner IP enregistre la liste des serveurs ;
- L'observateur d'hôte exploite la liste.

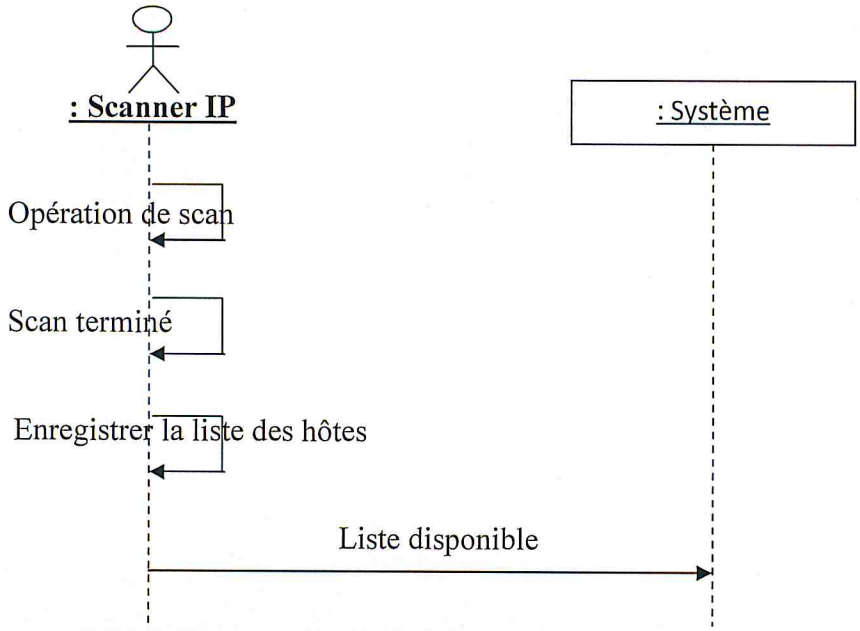


Fig.26. diagramme de séquence de Création de groupe de serveurs accessibles

VII.3.2 Demande de connexion

Dans ce cas d'utilisation les actions suivantes s'exécutent :

- L'administrateur déclenche l'opération de demande de connexion au serveur ;
- Le système lui demande l'adresse IP du serveur, le nom utilisateur et le mot de passe, via une interface de saisie ;
- L'administrateur sélectionne un serveur, à partir d'une liste établit par le scanner IP ;
- L'administrateur saisi, un nom utilisateur et un mot de passe ;
- Le système demande l'établissement de la connexion avec le serveur.

VII.3.3. Authentification

L'authentification s'exécute selon les actions suivantes :

- Le serveur reçoit la demande d'établissement d'une connexion ;
- Le serveur valide le nom et le mot de passe ;
- Si la validation est terminée avec succès, le serveur crée une session pour cet utilisateur, sinon la connexion est refusée.

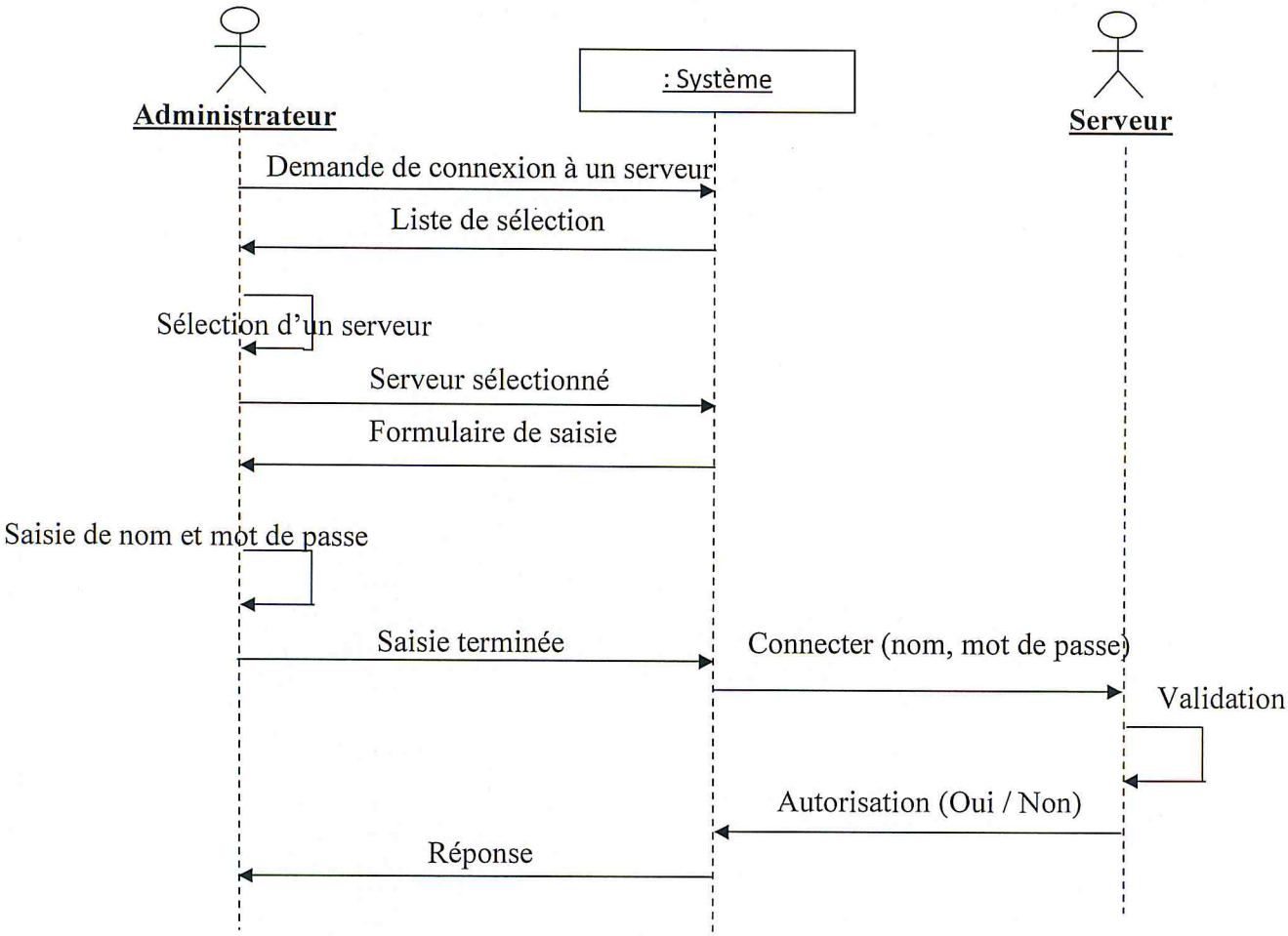


Fig.27. diagramme de séquence de Connexion au serveur

VII.3.4. Lister les partages de tout le réseau

Ce cas d'utilisation comporte les actions suivantes :

- L'administrateur déclenche la fenêtre de observateur des ressources partagées ;
- le système lui répond par un formulaire de saisie le nom d'utilisateur et le mot de passe;
- L'administrateur saisie le nom d'utilisateur et le mot de passe;
- Le système demande l'établissement de la connexion avec le serveur.
- Si la validation est terminée avec succès, le système affiche tous les partages de réseau sinon la connexion est refusée.

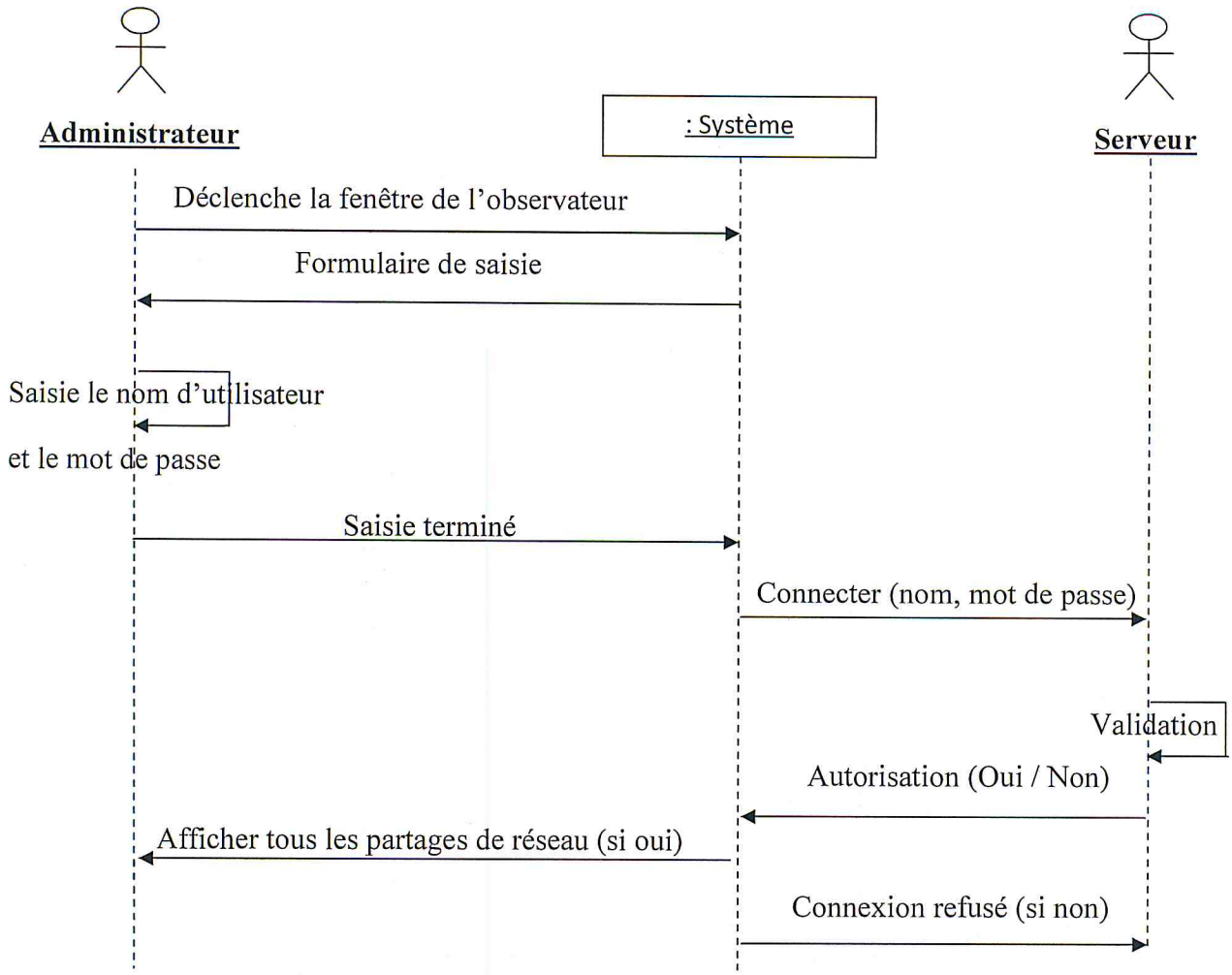


Fig.28. diagramme de séquence pour lister les partages de tous le réseau

VII.4. Description des collaborations

VII.4.1. Authentification

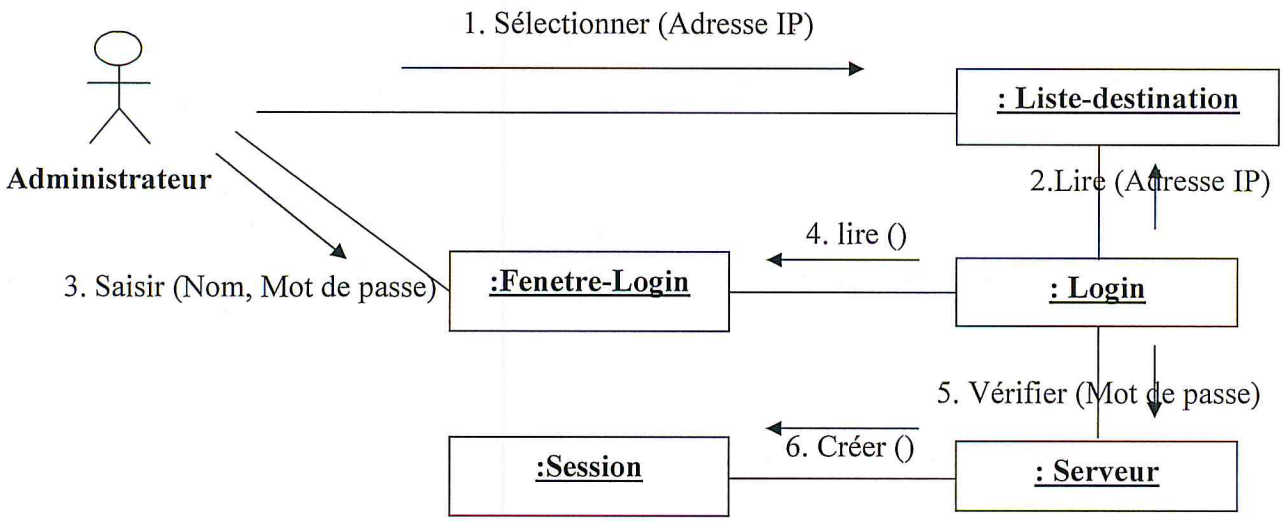


Fig.29.Réalisation de validation d'authentification par collaboration entre objets

VII.5. Diagramme de classes de l'Observateur des ressources partagées

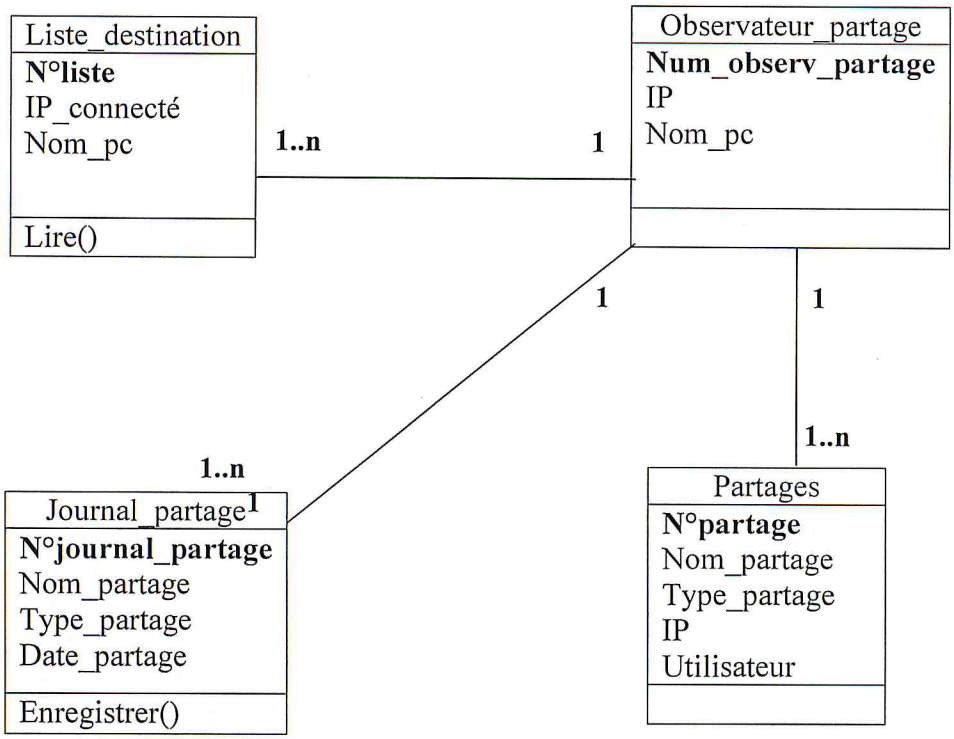


Fig.30.Diagramme de classes du système de l'observateur de partages

VIII. DIAGRAMME DE CLASSES FINAL DE L'OUTIL DE SURVEILLANCE DES RESSOURCES PARTAGÉES

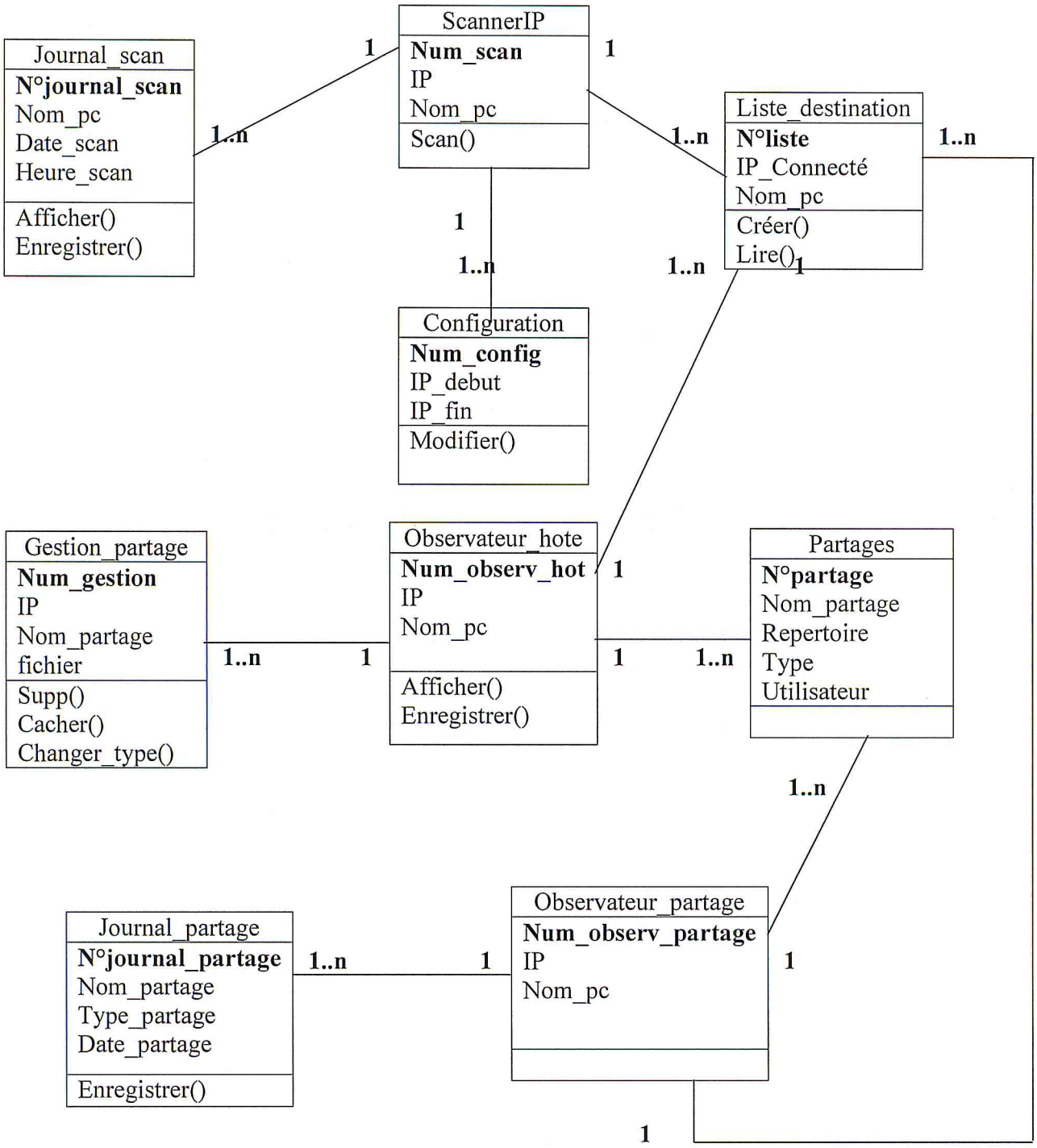


Fig.31.Diagramme de classe final de l'outil de surveillance des ressources partagées

IX. Journalisation

L'audit est un procédé de sécurité très fiable dans la mesure où il permet de recenser tout ce qui se passe au sein d'un système et de prévenir toute activité suspecte le concernant. Dans notre cas, il s'agit de surveiller les accès aux différentes ressources partagées pour permettre aux administrateurs de connaître à tout instant les ressources partagées (type de ressource, accès aux ressources, utilisateur courant,…etc.) et prendre les décisions nécessaires à l'encontre des failles et problèmes observés. Cela ne peut être réalisé que si on met en place le système d'audit adéquat. Dans le cadre de notre projet, ça sera la mise en place d'une base de données dans laquelle toutes les informations récupérées sont enregistrées pour permettre aux administrateurs de revenir sur l'historique des accès aux partages via un formulaire journal.

La base de données est constituée de trois tables :

Partage : (adresse IP, ressource partagée, type de partage, type d'accès, utilisateurs, date, heure).

Session : (adresse IP, nom utilisateur, temps d'activité, temps d'inactivité, date, heure).

Scanner : (adresse IP, nom poste, date scan, heure scan).

Chapitre IV

Implémentation

I. ENVIRONNEMENT DE DÉVELOPPEMENT

I.1. Langage de programmation JAVA

Langage de développement, produit par la société Sun et lancé le 23 mai 1995. Ecrit par James Gosling, il permet de créer des applications autonomes et de doter les documents html de nouvelles fonctionnalités : animations interactives, applications intégrées, modèles 3D, etc. Ce langage est orienté objet et comprend des éléments spécialement conçus pour la création d'applications multimédia. On écrit un programme java dans un texte source qui ressemble à C (langage) ou à C++, puis on le traduit à l'aide d'un compilateur afin de générer un programme utilisable directement dans une page html et appelé applet. Pour exécuter ensuite un applet, l'utilisateur doit disposer d'une machine virtuelle. Un applet est inclus sous forme de document html ou sous forme de hyperlink. [7]

I.2.SGBD ORACLE

Oracle est un SGBD (système de gestion de bases de données) édité par la société du même nom (Oracle Corporation - http://www.oracle.com), leader mondial des bases de données. La société *Oracle Corporation* a été créée en 1977 par Lawrence Ellison, Bob Miner, et Ed Oates. Elle s'appelle alors *Relational Software Incorporated (RSI)* et commercialise un Système de Gestion de Bases de données relationnelles (SGBDR ou RDBMS pour *Relational Database Management System*) nommé*Oracle*.

Permettant d'assurer :

- La définition et la manipulation des données
- La cohérence des données
- La confidentialité des données
- L'intégrité des données
- La sauvegarde et la restauration des données
- La gestion des accès concurrents. [8]

I.3.Protocol SMB

SMB, pour "Server Message Block", est un protocole réseau destiné à permettre le partage de fichiers entre différents périphériques connectés au même réseau informatique.

Principalement utilisé sur les réseaux informatiques locaux, le **SMB** repose sur le principe d'un périphérique serveur qui héberge les fichiers à partager et d'un périphérique client qui va envoyer des requêtes au serveur dans le but d'accéder aux fichiers stockés à distance.

Par exemple, un disque dur multimédia implémentant le protocole **SMB** permet de lire les fichiers compatibles qui sont stockés sur un ordinateur lorsque tous deux sont connectés au même réseau. [9]

II. OUTIL DE SURVEILLANCE DES RESSOURCES PARTAGÉES

II.1. Présentation générale

Les documents de notre application sont :

1. Un scanner IP ;
2. Un observateur des ressources partagées ;
3. Un observateur d'hôte ;
4. Des journaux d'événements.

Le menu principal permet à l'utilisateur d'exécuter plusieurs fonctionnalités liées aux différentes fenêtres. La barre d'outil offre un moyen simple d'organiser et de gérer des contrôles visuels les boutons d'outils correspondants aux éléments de menus de l'application et ils permettent à l'utilisateur d'accéder d'une manière plus directe aux commandes de l'application.

L'exécution de l'application commence tout d'abord par le lancement de l'outil scanner IP.

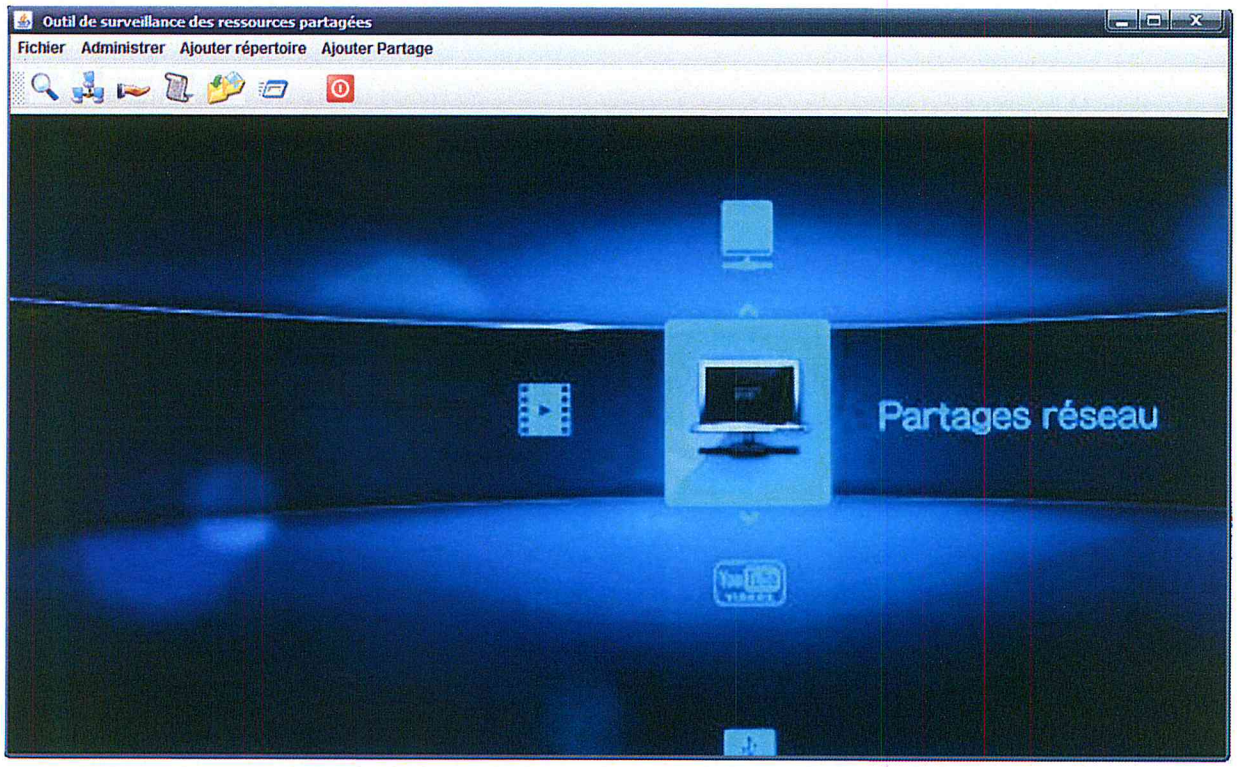


Fig.32.Interface principale de l'application « outil de surveillance des ressources partagées sur un réseau local Microsoft »

II.2. Présentation détaillée de chaque interface

II.2.1. Authentification d'application

L'utilisateur doit saisi leur nom et le mot passe correcte pour accès aux modules de l'application sinon un message d'erreur sera affiché.

Fig.33.Fenêtre d'authentification

II.2.2. Scanner IP

Cette fenêtre constitue l'outil scanner IP, cet outil permet à un utilisateur de recenser toutes les machines accessibles sur le réseau en cliquant sur le bouton «Scanner IP».

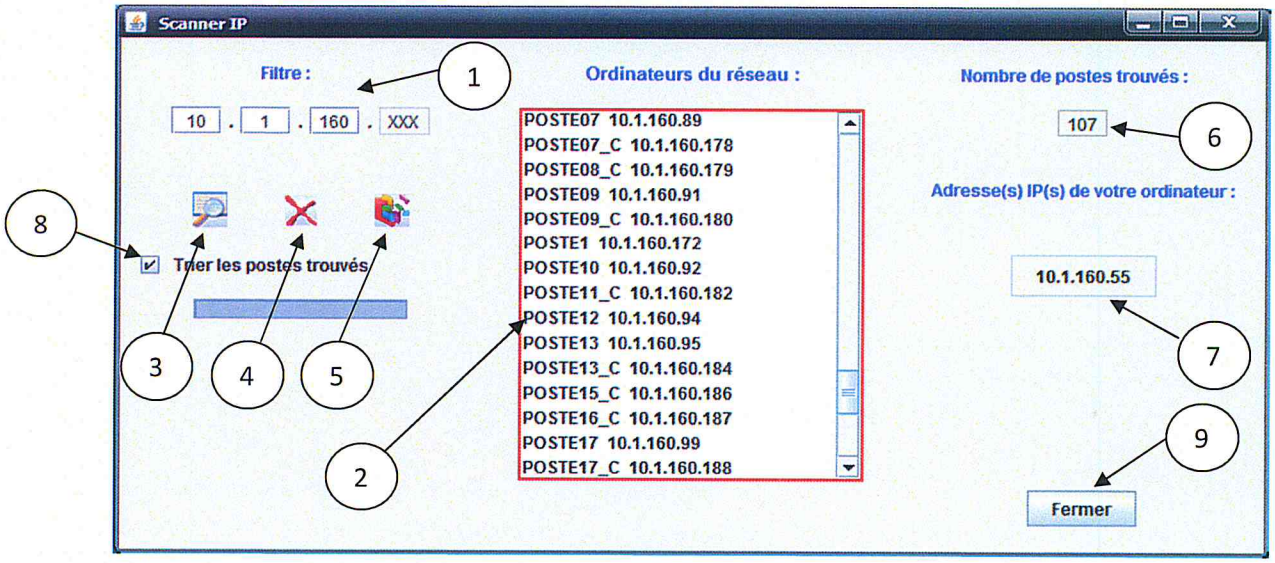


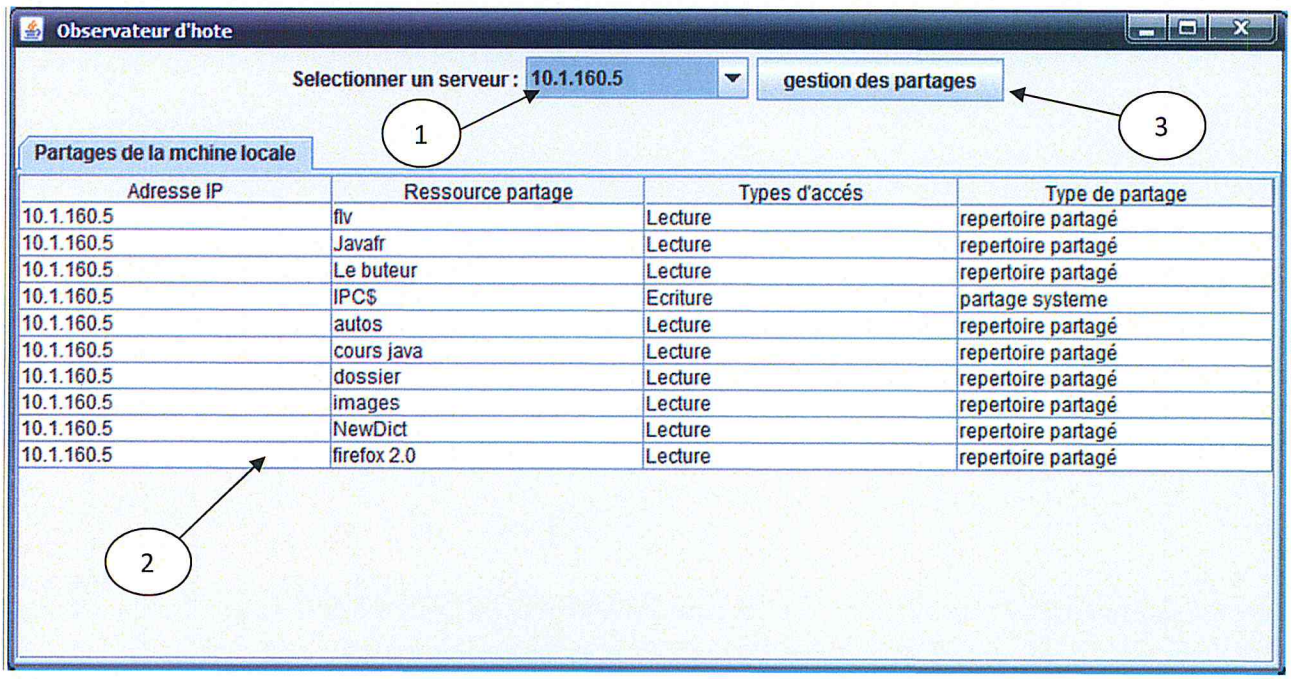
Fig.34.Fenêtre de Scanner IP

Les différents contrôles du scanner IP sont:

1. La plage de scan IP : permet a l'utilisateur de modifié l'intervalle de scan sauf le dernier octet de l'adresse IP est variés par défaut entre 1 et 254.
2. La liste d'affichage des différentes informations récupérées telles que : (l'adresse IP et le nom machine)
3. Démarrer l'opération de scan ;
4. effacer la liste : Initialisation de la liste d'affichage ;
5. Trier la liste par ordre alphabétique.
6. Compter le nombre des postes trouvés.
7. L'adresse IP de la machine locale, fournit par le scanner, elle indique l'adresse IP de la machine locale ;
8. Trier automatiquement la liste des postes scannées par ordre alphabétique après chaque recherche.
9. Quitter la fenêtre de scanner IP.

II.2.3. Observateur des partages par hôte

L'observateur est accessible via le menu principal en cliquant sur le bouton « Observer par hôte». L'observateur contient au départ toutes les informations concernant la machine locale,



Adresse IP	Ressource partage	Types d'accés	Type de partage
10.1.160.5	flv	Lecture	repertoire partagé
10.1.160.5	Javafr	Lecture	repertoire partagé
10.1.160.5	Le buteur	Lecture	repertoire partagé
10.1.160.5	IPC$	Ecriture	partage systeme
10.1.160.5	autos	Lecture	repertoire partagé
10.1.160.5	cours java	Lecture	repertoire partagé
10.1.160.5	dossier	Lecture	repertoire partagé
10.1.160.5	images	Lecture	repertoire partagé
10.1.160.5	NewDict	Lecture	repertoire partagé
10.1.160.5	firefox 2.0	Lecture	repertoire partagé

Fig.35.Fenêtre de l'observateur des partages par hôte

Cette fenêtre contient toutes les informations concernant les ressources partagées sur un hôte telles que :

1. Sélectionner un serveur : sélection de serveur a observé ces ressources partagées dans la liste des hôtes déroulantes.
2. Anglet « partages de la machine locale » : contient des informations concernant les ressources partagées de la machine locale telle que :

- Ressource partagée : affiche le nom de la ressource partagée sur l'hôte ;
- Type de partage : Une ressource partagée peut être :
  - ✓ Un répertoire partagé ;
  - ✓ Un canal nommé ;
  - ✓ Une imprimante partagée ;
  - ✓ Spécial créé par le système permet au personnel administratif de se connecter au répertoire racine d'un périphérique de stockage ;
  - ✓ Une ressource d'un type non reconnu ;
- Type d'accès : les types d'autorisations d'accès qui peuvent être appliqués aux dossiers partagés sont :
  - ❖ Lecture : l'autorisation Lecture permet :
  - ✓ L'affichage des noms de fichier et de sous-dossiers ;
  - ✓ Le parcours des dossiers et sous-dossier ;
  - ✓ L'affichage des contenus des fichiers ;
  - ✓ L'exécution des fichiers programme.
  - ❖ Modification : permettant la lecture, elle permet aussi :
  - ✓ L'ajout et la création de fichiers et de sous-dossiers ;
  - ✓ La modification des fichiers ;
  - ✓ La suppression de sous-dossiers et de fichiers.
  - ❖ Contrôle total : le contrôle total est l'autorisation par défaut appliquée à tous les partages. Incluant la lecture et la modification, elle permet aussi :
  - ✓ La modification des autorisations (uniquement pour les fichiers et dossiers NTFS) ;
  - ✓ L'appropriation (uniquement des fichiers et dossiers NTFS).

3. bouton « gestion des partages » : permet de supprimer, cacher et changer le type d'accès d'un répertoire ou un fichier le détail des fonctionnalités sera expliqué plus loin.

Pour afficher toutes ces informations concernant la ressource partagée nous avons utilisé le protocole SMB, qui permet de récupérer la liste des partages, leurs types, l'adresse de partage etc.

L'observateur de partages offre aussi à l'utilisateur la possibilité d'afficher les ressources partagées d'un hôte, on sélectionne l'hôte à partir d'une liste établie par le scanner IP. Lorsque en fait la sélection une fenêtre d'authentification sera affiché, l'administrateur doit saisie le nom d'utilisateur et le mot de passe de cet hôte pour permettre d'afficher ces partages

Fig.36.Authentification serveur

Si le nom d'utilisateur et le mot de passe saisie sont corrects alors, toutes les informations concernant la machine dont l'adresse IP est indiquée sur le titre de l'anglet crée nouvellement.

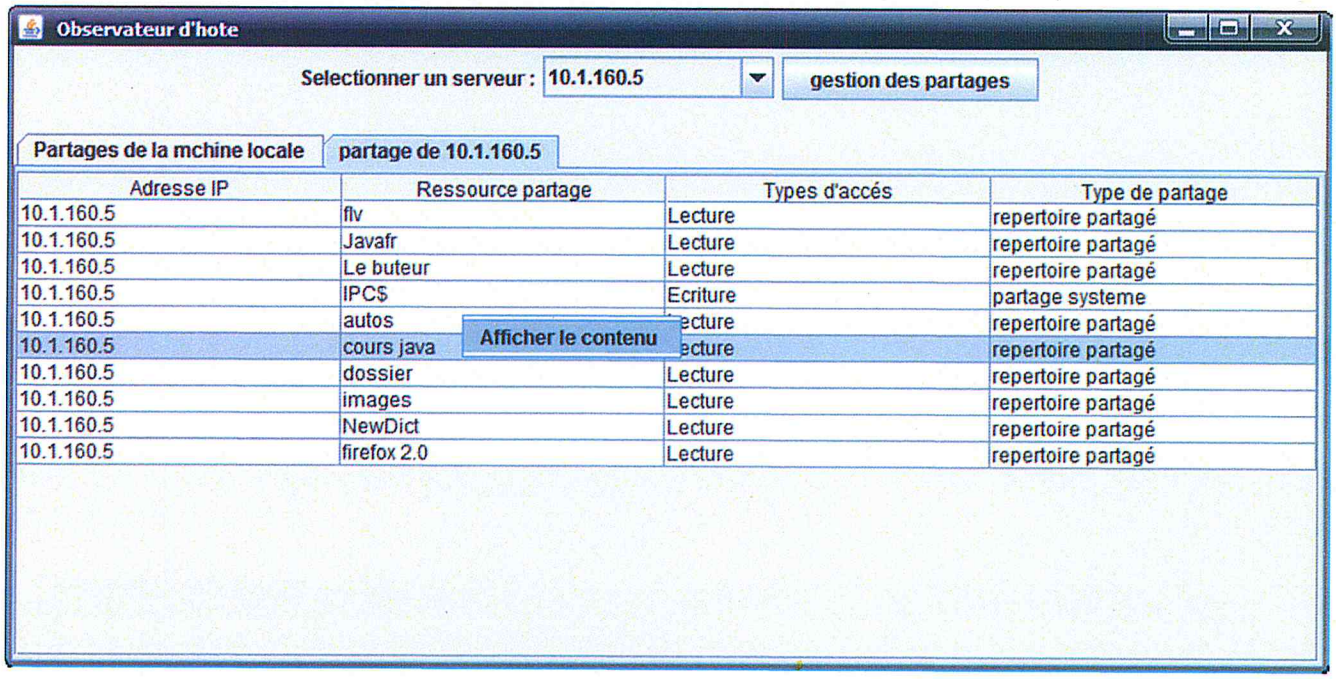
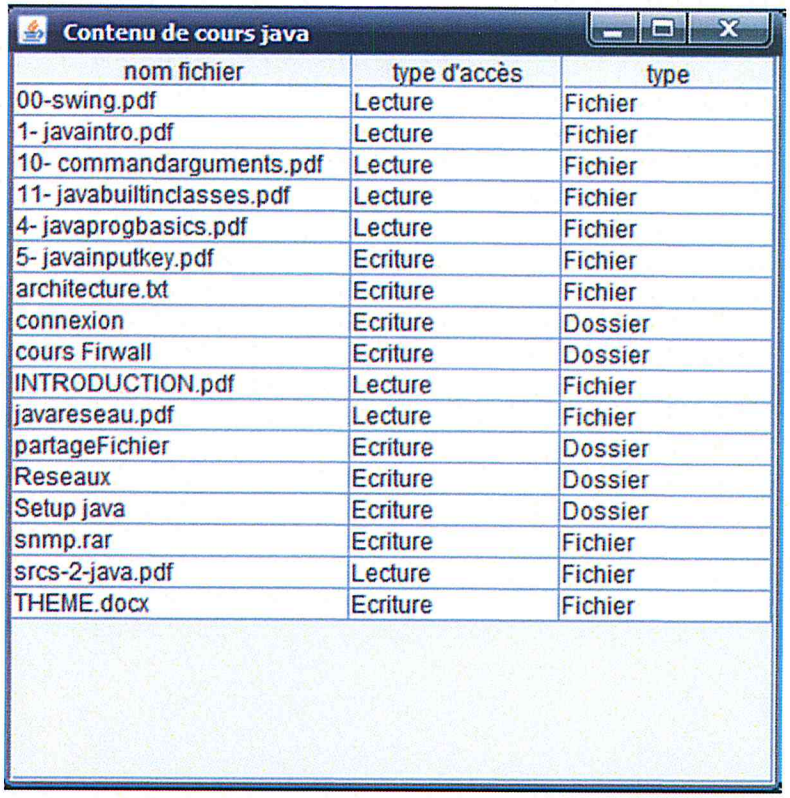


Fig.37.Fenêtre observateur par hôte

L'utilisateur peut aussi afficher le contenu d'un partage par un clic à droite « afficher le contenu » sur un partage choisi, une fenêtre ci-dessus sera affichée, dans ce cas on a choisi le dossier partagé « cours java ».



nom fichier	type d'accès	type
00-swing.pdf	Lecture	Fichier
1- javaintro.pdf	Lecture	Fichier
10- commandarguments.pdf	Lecture	Fichier
11- javabuiltinclasses.pdf	Lecture	Fichier
4- javaprogbasics.pdf	Lecture	Fichier
5- javainputkey.pdf	Ecriture	Fichier
architecture.txt	Ecriture	Fichier
connexion	Ecriture	Dossier
cours Firwall	Ecriture	Dossier
INTRODUCTION.pdf	Lecture	Fichier
javareseau.pdf	Lecture	Fichier
partageFichier	Ecriture	Dossier
Reseaux	Ecriture	Dossier
Setup java	Ecriture	Dossier
snmp.rar	Ecriture	Fichier
srcs-2-java.pdf	Lecture	Fichier
THEME.docx	Ecriture	Fichier

Fig.38.Fenêtre de contenu d'un dossier partagé

Cette fenêtre contient des informations concernant les documents de partage choisi à voir leur contenu telles que :

- Nom de fichier : affiche le nom de document
- Type d'accès : affiche le type d'accès de fichier ou document (lecture, écriture)
- Type : affiche le type de contenu telle que dossier ou fichier ou cacher.

II.2.3.1. Gestion des partages

L'administrateur peut aussi supprimer, cacher, changer le type d'accès de répertoire ou de fichier sélectionné. Cette opération n'est permise qu'à l'administrateur de l'hôte cible, après l'ouverture d'une session administrateur sur l'hôte sélectionné. L'observateur des hôtes assure cette fonctionnalité en choisissant «Gestion des partages », la fenêtre de gestion des partages illustré par cette figure.

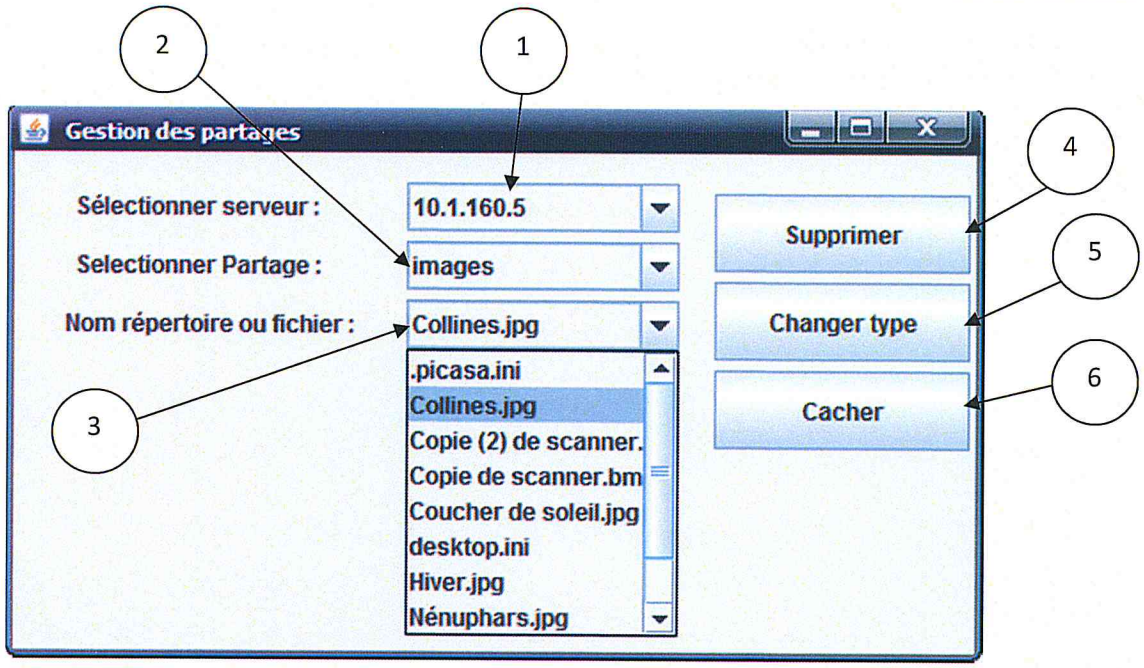


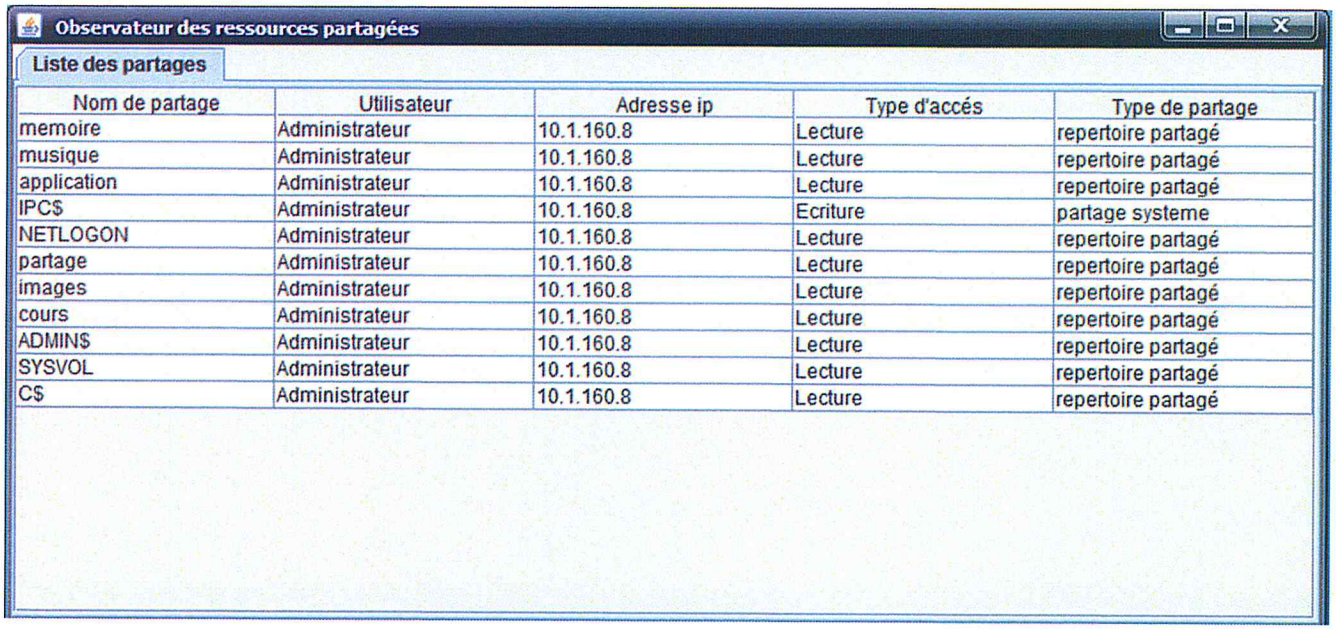
Fig.39.Fenêtre de gestion des partages

Cette fenêtre contient les paramètres suivants :

1. Sélectionner serveur : l'administrateur doit sélectionner un serveur pour obtenir la liste des partages de ce dernier.
2. Sélectionner partage : après la sélection de serveur, une liste des partages de ce serveur sera exploitée automatiquement, toujours l'administrateur doit sélectionner le partage qui contient le fichier que nous voulons gérer.
3. Nom répertoire ou fichier : tant que l'administrateur a sélectionné un dossier partagé une liste de contenu de ce dossier sera affiché toujours automatiquement.
4. Bouton « supprimer » : supprime le répertoire ou fichier sélectionné.
5. Bouton « changer type » : permet de changer le type d'accès de fichier sélectionné.
6. Bouton « Cacher » : permet de cacher le répertoire ou fichier sélectionné.

II.2.4. Observateur des ressources partagées

Cet outil permet à l'administrateur de voir toutes les dossiers partagées de toutes les machines accessible de réseau en temps réel.

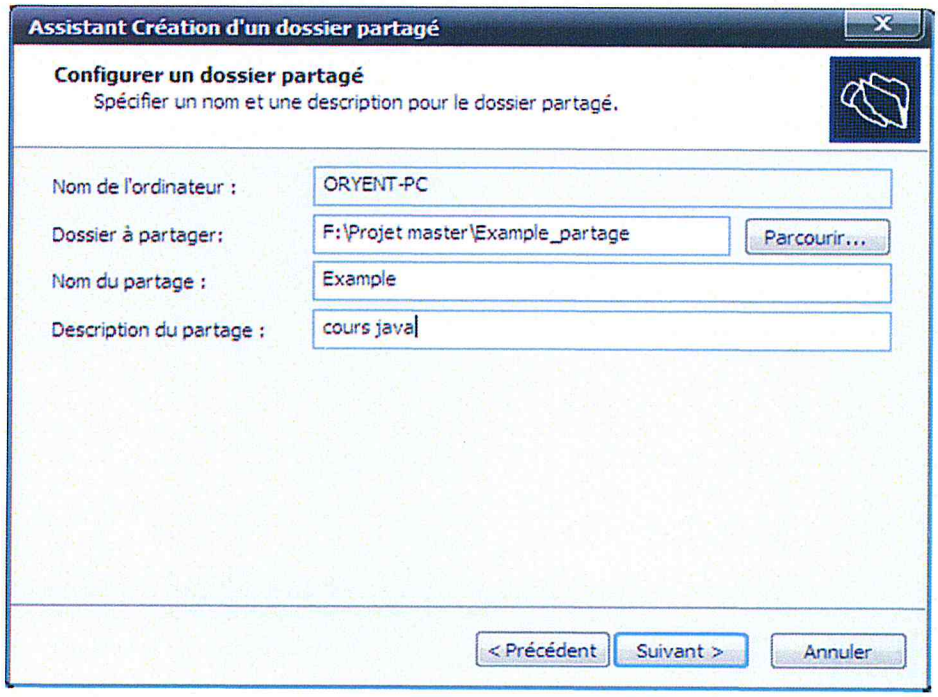


Nom de partage	Utilisateur	Adresse ip	Type d'accés	Type de partage
memoire	Administrateur	10.1.160.8	Lecture	repertoire partagé
musique	Administrateur	10.1.160.8	Lecture	repertoire partagé
application	Administrateur	10.1.160.8	Lecture	repertoire partagé
IPC$	Administrateur	10.1.160.8	Ecriture	partage systeme
NETLOGON	Administrateur	10.1.160.8	Lecture	repertoire partagé
partage	Administrateur	10.1.160.8	Lecture	repertoire partagé
images	Administrateur	10.1.160.8	Lecture	repertoire partagé
cours	Administrateur	10.1.160.8	Lecture	repertoire partagé
ADMIN$	Administrateur	10.1.160.8	Lecture	repertoire partagé
SYSVOL	Administrateur	10.1.160.8	Lecture	repertoire partagé
C$	Administrateur	10.1.160.8	Lecture	repertoire partagé

Fig.40.Fenêtre d'observateur des ressources partagées

II.2.5. Ajouter nouveau partage

Notre application offre aussi la possibilité d'ajouter un nouveau partage en cliquant sur le bouton «Nouveau partage » dans la barre d'outils, cette opération n'est permise qu'à l'administrateur de l'hôte cible, ce dernier doit ajouter le chemin complet de la ressource à partager ainsi que le nom, une description du partage les autorisations d'accès à cette ressource comme illustre les deux figures suivantes :



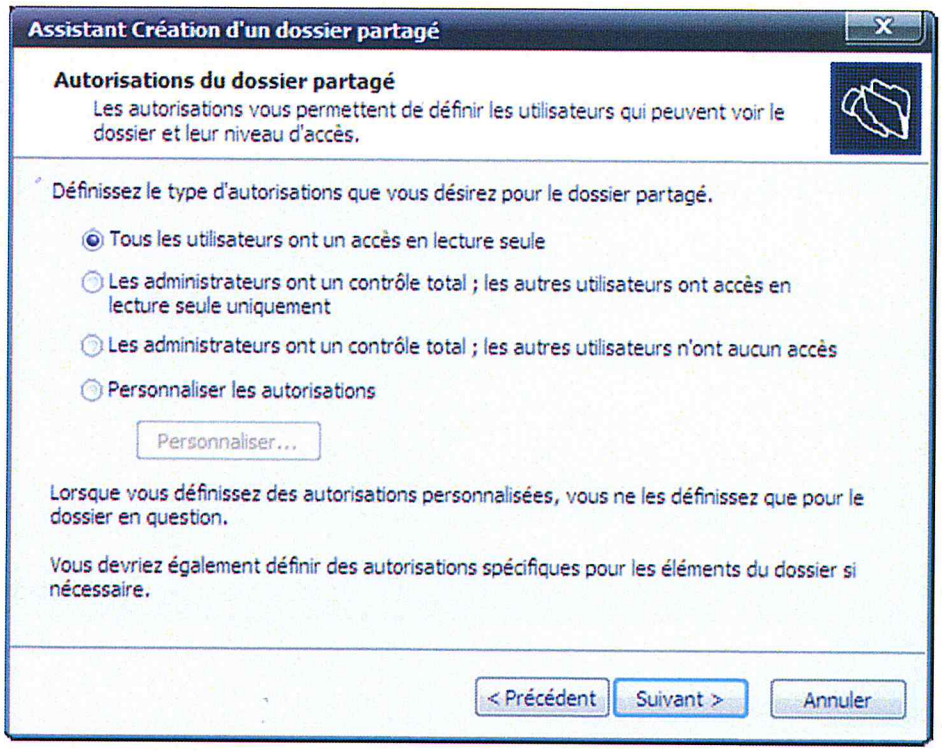


Fig.41.Fenêtre de l'Assistant création d'un dossier partagé

II.2.6. Ajouter nouveau répertoire dans un dossier partagé

Cet outil permet à l'utilisateur d'ajouter un répertoire dans un dossier partagé

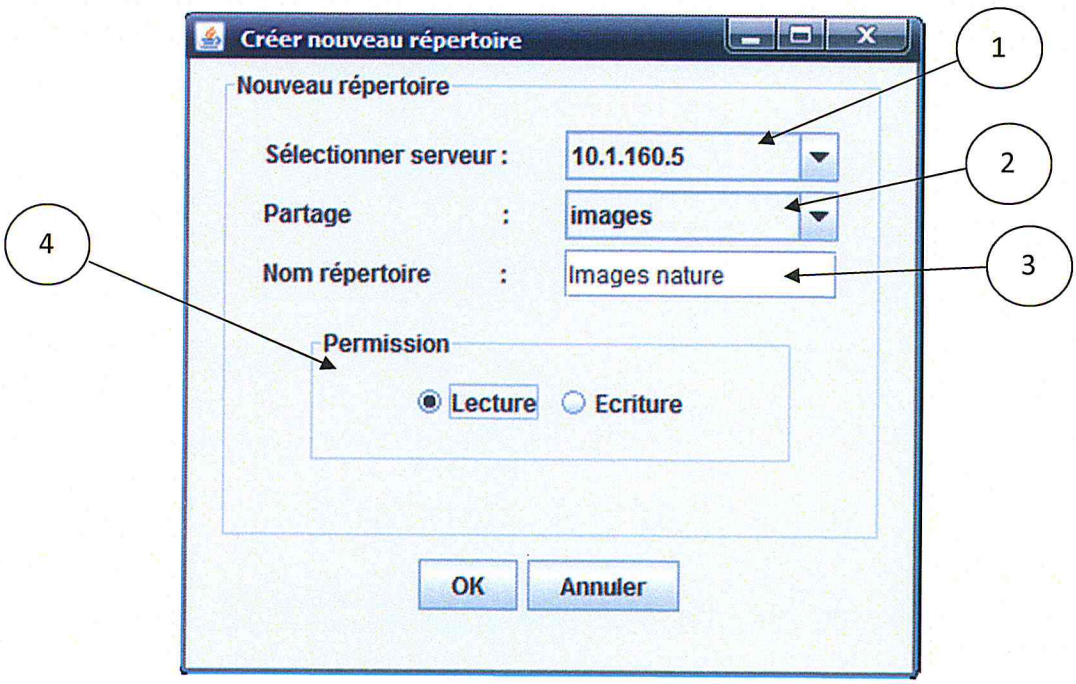


Fig.42.Fenêtre de création de nouveau répertoire dans un partage

Cette fenêtre contient les paramètres suivants :

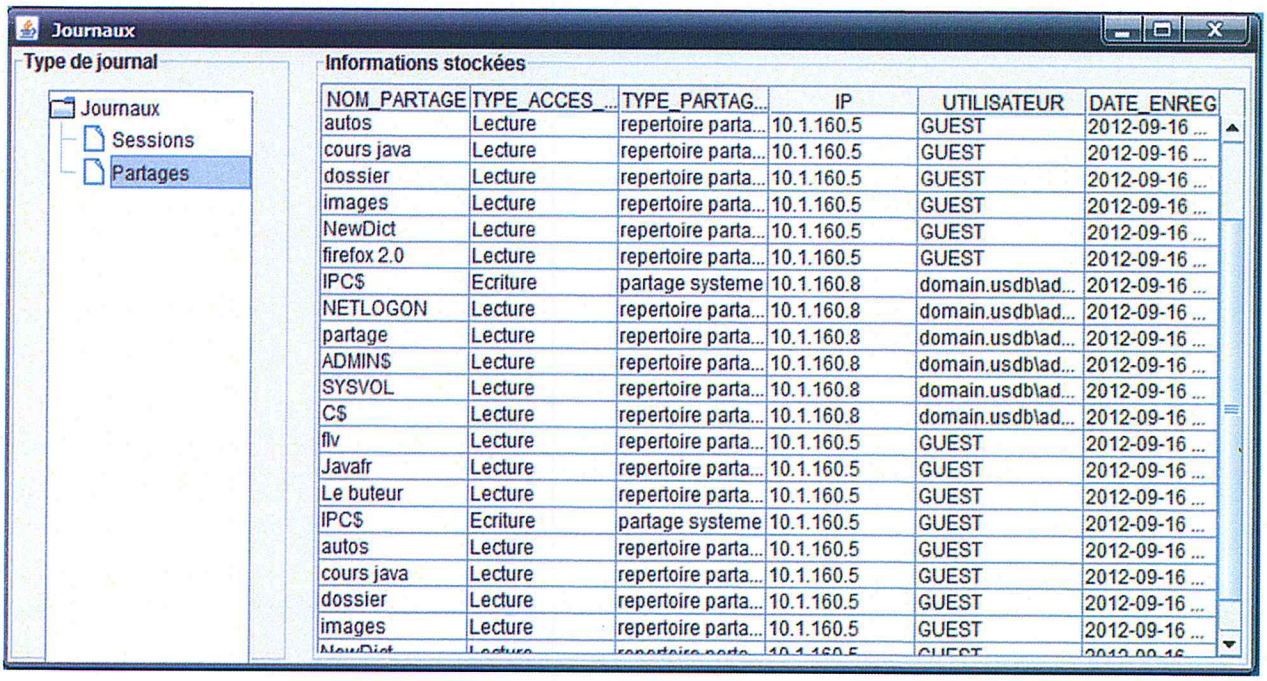
1. Sélectionner serveur : permet de l'administrateur a spécifié un serveur.
2. Partage : une liste des partages de serveur sélectionné sera affichée par conséquent, l'administrateur spécifier le partage que doit l'insérer le nouveau répertoire.
3. Nom de répertoire : l'administrateur doit donner un nom de répertoire a ajouté.
4. Permission : l'administrateur doit spécifier le type d'accès de répertoire (lecture ou écriture).

II.2.7. Journaux des évènements

Les journaux sont un élément très important pour l'activité de surveillance, ils permettent à l'administrateur de revenir sur les anciennes partages. Pour cela, nous avons adopté une procédure de sauvegarde de toutes les informations récupérées par notre système. La sauvegarde comporte les informations essentielles telles que :

- Journal des ressources partagées sur le réseau local par machine ;
- Journal des différentes sessions ouvertes sur une machine ;

La figure suivante montre un exemple de journal.



NOM_PARTAGE	TYPE_ACCES_...	TYPE_PARTAG...	IP	UTILISATEUR	DATE_ENREG
autos	Lecture	repertoire parta...	10.1.160.5	GUEST	2012-09-16 ...
cours java	Lecture	repertoire parta...	10.1.160.5	GUEST	2012-09-16 ...
dossier	Lecture	repertoire parta...	10.1.160.5	GUEST	2012-09-16 ...
images	Lecture	repertoire parta...	10.1.160.5	GUEST	2012-09-16 ...
NewDict	Lecture	repertoire parta...	10.1.160.5	GUEST	2012-09-16 ...
firefox 2.0	Lecture	repertoire parta...	10.1.160.5	GUEST	2012-09-16 ...
IPC$	Ecriture	partage systeme	10.1.160.8	domain.usdb\ad...	2012-09-16 ...
NETLOGON	Lecture	repertoire parta...	10.1.160.8	domain.usdb\ad...	2012-09-16 ...
partage	Lecture	repertoire parta...	10.1.160.8	domain.usdb\ad...	2012-09-16 ...
ADMIN$	Lecture	repertoire parta...	10.1.160.8	domain.usdb\ad...	2012-09-16 ...
SYSVOL	Lecture	repertoire parta...	10.1.160.8	domain.usdb\ad...	2012-09-16 ...
C$	Lecture	repertoire parta...	10.1.160.8	domain.usdb\ad...	2012-09-16 ...
flv	Lecture	repertoire parta...	10.1.160.5	GUEST	2012-09-16 ...
Javafr	Lecture	repertoire parta...	10.1.160.5	GUEST	2012-09-16 ...
Le buteur	Lecture	repertoire parta...	10.1.160.5	GUEST	2012-09-16 ...
IPC$	Ecriture	partage systeme	10.1.160.5	GUEST	2012-09-16 ...
autos	Lecture	repertoire parta...	10.1.160.5	GUEST	2012-09-16 ...
cours java	Lecture	repertoire parta...	10.1.160.5	GUEST	2012-09-16 ...
dossier	Lecture	repertoire parta...	10.1.160.5	GUEST	2012-09-16 ...
images	Lecture	repertoire parta...	10.1.160.5	GUEST	2012-09-16 ...

Fig.43. Fenêtre journaux

CONCLUSION GÉNÉRALE

Le travail effectué dans ce projet fait partie du domaine de la sécurité informatique, et joue le rôle d'un complément à d'autres outils de sécurité et de surveillance des réseaux informatiques car la sécurité informatique est un domaine très vaste et varié. C'est pour cette raison qu'actuellement plusieurs moyens de sécurité sont combinés pour répondre aux nouvelles exigences de sécurité.

Ce projet nous a permis d'acquérir des connaissances approfondies dans le domaine des réseaux informatiques, de connaître et de manipuler quelques fonctionnalités des protocoles de communication, ainsi que le fonctionnement des sockets, sur lesquelles se base les différentes communications.

Aussi de mieux appliquer les principes et les méthodes théoriques de conception dispensés durant notre cursus de Master, en l'occurrence, la conception et la programmation orientée objet, les systèmes d'exploitations et les réseaux informatiques.

D'un autre point de vue, ce projet nous a permis de nous familiariser avec un langage de programmation puissant et ouvert, à savoir le JAVA.

D'autres actions en perspective peuvent être accomplies pour compléter ce travail :

- Compléter les différentes fonctionnalités d'administration manquantes par rapport à un outil de gestion d'un ordinateur.
- Étendre les différentes fonctionnalités offertes par notre application à d'autres systèmes d'exploitation.
- ...

RÉFÉRENCES

BIBLIOGRAPHIE :

[1] Les Réseaux Informatiques D. Lalot

[2] Supervision réseau Auteur COPONAT Pierre-Adrien, REYNIER Serge

[3] La gestion réseau et le protocole SNMP Aurélien Méré FIIFO4

[4] Modélisation objet avec UML, Pierre Alain Muller, 1997.

WEBOGRAPHIIE :

[5] http://www.CommentCaMarche.com

[6] http://www.WindowServer.com

[7] http://DicoFR.com

[8] http://cours-dba-oracle.blogspot.com/p/architecture.html

[9] http://www.homecine-compare.com/definition-de-smb.htm