

Signature de l'encadrant (LINAGORA)

Sami BOUHLEL

Signature du superviseur (ESPRIT)

Mr. Mohamed Aymen BEN CHEIKHA

Résumé

LE document présent est le résumé de mon travail dans le cadre du projet de fin d'étude au sein de l'entreprise LINAGORA.

Le but de ce projet est la mise en place d'un identifiant numérique unique pour chaque citoyen et la mise en place d'une solution d'authentification centralisée pour le gouvernement Tunisien.

Mots clés : OpenLDAP, Authentification, LinID, WebSSO.

Abstract

This document is a summary of our work in the project end of study within the company LINAGORA

The purpose of this project is the establishment of a unique numeric identifier for every Tunisian citizen and the Deployment of a centralized authentication solution for the Tunisian government.

Keywords : Directory, Authentification, LinID, WebSSO.

Remerciements

Avant tout développement sur cette expérience professionnelle, j'aimerais commencer ce rapport de stage par des remerciements, à ceux qui m'ont apporté leurs soutiens et qui m'ont beaucoup appris au cours de ce stage au sein de LINAGORA TUNISIE, et à tous les membres de l'équipe LINAGORA FRANCE.

Je remercie M.Sami Bouhlef, mon maitre de stage qui m'a formé et accompagné tout au long de cette expérience professionnelle avec beaucoup de patience et de pédagogie. Je salue également l'ensemble de l'équipe support de Linagora pour les conseils qu'ils ont pu me prodiguer au cours de ces quatre mois.

Je remercie chaleureusement Mr Mohamed Aymen BEN CHEIKHA, David Coutadeur, Alexandre Chapelon et M.Amine Bouhlef, sans qui ce stage n'aurait pas été un moment aussi profitable.

Table des matières

Introduction Générale	2
1 Présentation du stage	3
1.1 Cadre du projet	3
1.2 Présentation de l'organisme d'accueil	3
Linagora	3
LINAGORA, premier EOS	5
Produits	5
1.3 Projet : Mise en place d'un identifiant numérique unique pour chaque citoyen	6
1.4 Présentation de la mission du stage	7
Introduction	7
Mission de stage	7
Démarche du projet	7
1.5 Conclusion	8
2 Concepts Clés	9
2.1 Introduction	9
2.2 LDAP	9
Definition d'un annuaire	9
Historique du Protocole	9
Les models de LDAP	10
Que peut apporter LDAP ?	13
Différence entre une base de donnée et un annuaire	13
2.3 LSC : LDAP Synchronization Connector	14
2.4 WebSSO [Single-Sign-On]	14
Definition	14
2.5 Protocole HTTP	16
Présentation	16
HTTP - Requête	16
HTTP - Réponse	16
HTTP - Cookie	16
2.6 Conclusion	17

3	Spécifications des besoins	18
3.1	Introduction	18
3.2	Analyse des besoins	18
	Les objectifs du projet	18
	Besoins fonctionnels	18
	Besoins non fonctionnels	19
3.3	Vue fonctionnelle du système	19
	Identification des acteurs	19
	Cas d'utilisation global	20
	Raffinement du cas d'utilisation « Recherche »	21
	Diagramme de sequence système de cas d'utilisation « re- cherche avancée employé »	22
	Raffinement du cas d'utilisation « Navigation »	23
	Diagramme de sequence système de cas d'utilisation « Navigation par type » :	24
	Diagramme de Collaboration de cas d'utilisation « Navigation par type »	25
3.4	Vue technique du système	26
	Spécification des Besoins techniques	26
	Spécification de l'annuaire centralisé	27
3.5	Conclusion	27
4	Conception de l'annuaire et Architecture	28
4.1	Introduction	28
4.2	Annuaire LDAP	28
	Structure d'annuaire	28
	Schéma d'annuaire	29
4.3	Architecture de la solution	34
	Architecture réseaux globale	34
	Conclusion	37
5	Réalisation du Projet	38
5.1	Introduction	38
5.2	Environnement de travail	38
	Environnement matériel	38
	Environnement logiciel	39
5.3	Taches réalisées	41
	Implémentation et configuration du serveur d'annuaire	41
5.4	Navigation à travers LinID	45
5.5	Conclusion	47
	Conclusion Générale	48
	Liste d'acronymes	49

Bibliographie	50
Netographie	51
Annexe	52

Table des figures

1.1	Presentation LINAGORA	4
1.2	Alternative aux logiciels propriétaires	6
2.1	Modèle d'information LDAP	10
2.2	Exemple de DIT	11
2.3	SSO par agent	14
2.4	SSO par délégation	15
2.5	SSO par mandataire inverse (reverse-proxy)	15
2.6	HTTP – Création d'un cookie	17
3.1	Diagramme de cas d'utilisation globale	20
3.2	Diagramme de Raffinement de cas d'utilisation « Recherche »	21
3.3	Diagramme de sequence de cas d'utilisation « Recherche avan- cée employé »	22
3.4	Diagramme de Raffinement de cas d'utilisation « Navigation »	23
3.5	Diagramme de sequence système de cas d'utilisation « Navi- gation par type »	25
3.6	Diagramme de Collaboration de cas d'utilisation « Navigation par type »	25
4.1	Structure d'annuaire	29
4.2	Architecture réseau globale	35
4.3	Specification Couche EDGE	36
5.1	OpenLDAP	39
5.2	Umbrello	40
5.3	Apache Directory Studio	40
5.4	Apache Web Server	41
5.5	configuration 1 du fichier slapd.conf	41
5.6	configuration 2 du fichier slapd.conf	42
5.7	Définition de la classe d'objet govStructure	42
5.8	Definition de la classe d'objet govPerson	43
5.9	Définition des attributs de govPerson	43
5.10	Definition des attributs de govStructure	44

5.11	Interface d'Apache DDirectory Studio	45
5.12	Interface d'accueil de LINID	46
5.13	Interface de Recherche d'une Personne	46
5.14	Interface de Recherche d'une Structure	47
5.15	Architecture matérielle	52
5.16	Matrice des flux	54
5.17	Partitionnement du serveur 1	55
5.18	Partitionnement du serveur 2	55
5.19	Portail de la plateforme	56
5.20	Menu des applications	57
5.21	Application OBM	57
5.22	Application Linshare	58

Liste des tableaux

4.1	Spécification de l'objet de classe Personne	30
4.2	Spécification de l'objet de classe Structure	31
4.3	Spécification de l'objet groupe dynamique	32
4.4	Spécification de l'objet groupe statique	33
4.5	Spécification de l'objet Applications	33
4.6	Spécification de l'objet Rôles applicatifs	34

Introduction Générale

L'économie en réseau ou la Net-économie est au cœur des débats et des stratégies de toutes les entreprises. Les organisations actuelles et les start-up tentent tous les jours de créer de nouveaux modèles en tirant parti des liens électroniques qu'elles peuvent tisser avec leurs clients, leurs partenaires et leurs fournisseurs.

Les perspectives sont immenses : elles concernent aussi bien la réduction des coûts de fonctionnement que la possibilité de générer de nouveaux revenus. Certaines entreprises ont réussi à économiser des dizaines, voire des centaines de millions de dinars par an à l'aide d'extranets, d'autres ont réussi à gagner de l'argent là où elles s'y attendaient le moins à l'aide de l'Internet.

De nouveaux métiers offerts par de nouveaux acteurs ont aussi trouvé leur place dans cette économie en réseau. Les places de marché électroniques, les sites de vente aux enchères, les sites communautaires, les portails ne sont que quelques exemples des opportunités qui se présentent. La créativité des hommes n'a pas de limites. Il y a des centaines de combinaisons et de modèles qui permettent d'apporter de la valeur aux consommateurs et aux entreprises.

L'un des principaux catalyseurs est indéniablement l'évolution des technologies informatiques et des réseaux. Au-delà de l'avènement du client léger grâce au navigateur Web, les technologies émergentes, comme LDAP, ont permis de résoudre des points essentiels, que nous décrivons ci-dessous et qui sont des facteurs clés de succès de la Net-économie. Le premier point a permis aux entreprises de réaliser des sites en ligne pouvant supporter un grand nombre d'utilisateurs et à moindre coût. L'économie en réseau nécessite la mise à disposition d'informations et de services aux clients, aux partenaires et aux fournisseurs d'une entreprise, disponibles dans son système d'information. Le nombre d'utilisateurs pouvant se connecter peut être très élevé. Une entreprise peut avoir des milliers, voire des millions de clients, qui peuvent se connecter à tout moment et de n'importe où. Le système d'information doit donc être en mesure de supporter cette charge et de s'adapter facilement à tout trafic supplémentaire. Il doit aussi assurer une qualité de service homogène quel que soit le nombre d'utilisateurs connectés. De plus, les services en ligne doivent tirer parti et s'intégrer avec les applications et les plates-formes existantes.

Il est donc nécessaire de réduire autant que possible l'impact que peut avoir sur celles-ci la connexion d'un grand nombre d'utilisateurs. Le deuxième point a donné aux entreprises la possibilité de personnaliser les informations publiées et les services offerts en fonction des profils de leurs clients, de leurs partenaires et de leurs fournisseurs. Plus il y a d'utilisateurs et plus les informations et les services offerts.

Dans ce contexte et dans le cadre de mise en œuvre des orientations nationales en matière de renforcement de l'utilisation des systèmes d'information nationales de service, le gouvernement Tunisien a mis comme objectif, l'instauration d'un système d'identification unique du citoyen.

Le Ministère de l'Enseignement supérieur et de la Recherche Scientifique et des Technologies de l'Information et de la Communication (Section Technologies de l'Information et de la Communication), chargé du projet, envisage de réaliser une étude globale et le déploiement d'un système national d'identification unique du citoyen, et ce dans le cadre d'un consensus entre les différents intervenants et tout en respectant les exigences relatives à la protection des données à caractère personnel.

Par la suite , et tout le long de ce rapport nous allons détailler cette étude en indiquant les étapes suivies afin de réaliser le projet.

Chapitre 1

Présentation du stage

Ce chapitre décrit la vue d'ensemble du projet, indique son cadre spatial, temporel, son contexte et énumère les concepts les plus importants liés à ce travail. Nous allons également introduire dans ce chapitre la méthodologie adoptée pour ce projet

1.1 Cadre du projet

Pour introduire ce projet, nous devons tout d'abord clarifier son objectif et les besoins qui ont fait apparaître la nécessité de le faire. Ce projet a été élaboré au sein de la société LINAGORA, pour une durée de 4 mois s'étalant du 22 Février 2016 au 22 juin 2016. Il a été réalisé dans le cadre de la présentation du projet de fin d'études, présenté en vue de l'obtention du d'ingénieur intégration Réseau et Télécommunications à l'école Supérieure Privée d'ingénierie et de Technologies pour l'année universitaire 2014/2015.

1.2 Présentation de l'organisme d'accueil

L'organisme qui représente le consommateur à qui ce travail est dédié, est Linagora et précisément l'équipe de l'intégration réseau et système.

Linagora

Linagora est un éditeur de Logiciel libre français, fondé en mai 2000 par Alexandre Zapolsky et Michel-Marie Maudet. Elle a été considérée comme un des leaders historiques européens du logiciel libre, en termes d'ingénierie, de conseil et de formation.

Linagora définit ses métiers en 4 grandes catégories :

- Linagora Global Software (LGS), sa vocation est de développer de nouveaux logiciels avec ses équipes de R/D et de les intégrer chez ses clients.
- Linagora Pro Services (LPS), une gamme de services professionnels qui vise à accompagner les grands utilisateurs de logiciels libres dans le projet de transformation de leur SI.
- Linagora Run Services (LRS), une gamme de services complète pour sécuriser votre Système d'information à composantes Open Source.
- Linagora Training Services (LTS), dont la mission est de réaliser un transfert de compétences full Open Source et de haut niveau pour ses clients.

Implanté en France mais aussi en Belgique, aux États-Unis (2008), au Canada (2013), au Vietnam (2015) et en Tunisie (2015)
Elle est à ce jour une des plus anciennes entreprises françaises dédiées aux logiciels libres toujours en activité. [N1]

Présentation de LINAGORA

Édition Logicielle

- OBM.com
- LinShare
- LinID
- petals
- LinPKi
- OpenPaaS

Assurance Logicielle

- OSSA

Services

- LINAGORA LINSTUDIO
- LINAGORA CONSULTING
- LINAGORA SERVICES
- LINAGORA FORMATION
- 15 ans LINAGORA

Quelques références LINAGORA

- UGAP
- Ministère de la Santé
- Ministère de la Défense
- SAGEM
- AFP
- EDF
- PSA PEUGEOT CITROËN
- ACCOR
- ORANGE
- SNCF
- BANQUE DE FRANCE
- Bouygues Telecom
- GIAL
- Inserm
- DGA
- CNES
- POLE EMPLOI
- LA CUB
- ASSEMBLÉE NATIONALE

150 salariés

Bureaux en France, Canada, Belgique, États Unis, Vietnam

Partenaires et clients en Tunisie, Colombie et au Nigéria

FIGURE 1.1 – Presentation LINAGORA

LINAGORA, premier EOS

Avec ses logiciels et services, LINAGORA permet aux grandes organisations publiques et privées de développer leur indépendance technologique

- Créateur des concepts SS2L (Société de Services en Logiciels Libres) et TM2L (Tierce Maintenance Logiciel Libre), LINAGORA se définit désormais comme un Éditeur Orienté Service (EOS).
- LINAGORA propose une Open Source Software Assurance (OSSA) sur 150 logiciels libres :
 - Prêts à l'industrialisation, sur une plate-forme unique : le 08000LINUX.com.
 - Avec garantie de service contractuelle : en cas de bug, LINAGORA s'engage au résultat sur des délais de résolution.
 - Gestion de la feuille de route du logiciel pour le compte du client et s'engage au reversement des développements.
- LINAGORA apporte également son expertise sur toute une gamme de services professionnels et de formations au travers de LINAGORA Formations à Paris et à Lyon.

Produits

Avec ses logiciels et services, LINAGORA permet aux grandes organisations publiques et privées de développer leur indépendance technologique

- **OBM**

Un logiciel Open Source de messagerie et de travail collaboratif, intégrant les meilleurs composants libres pour gérer et partager les informations au sein d'une organisation. OBM offre un périmètre fonctionnel riche et répond à de nombreux projets, simplement la meilleure alternative libre et gratuite. [N2]

- **LinID**

LinID est la seule suite logicielle de gestion d'identités complète Open Source, qui permet au clients de gagner en efficacité et en sécurité dans la gestion des données d'identité, d'accès et d'habilitation. [N3]

- **OpenPaaS**

une plate-forme de collaboration incluant des services de réseaux sociaux d'entreprise sous licence libre, c'est le fruit d'un projet de recherche bénéficiant du soutien du gouvernement français et faisant intervenir des partenaires issus de différents domaines. Il est conçu comme une plate-forme évolutive et déployable de manière éclatée sur plusieurs serveurs (pour obtenir performance et résilience) pouvant accueillir tout type d'application. [N4]

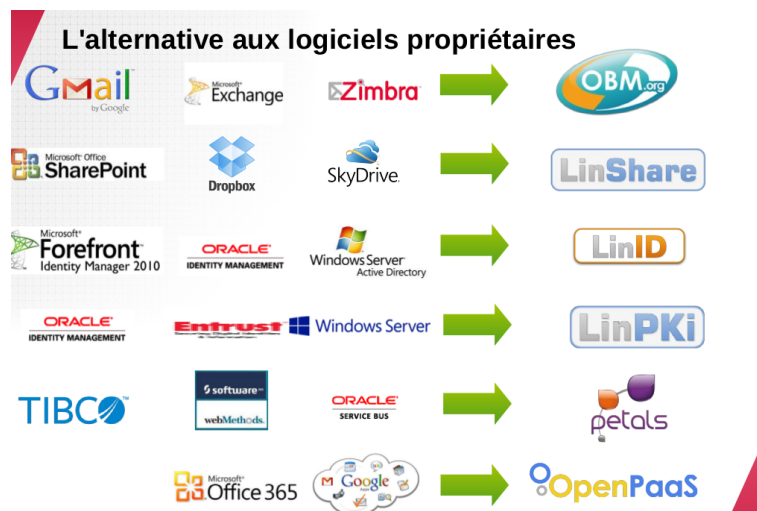


FIGURE 1.2 – Alternative aux logiciels propriétaires

1.3 Projet : Mise en place d'un identifiant numérique unique pour chaque citoyen

Dans le cadre de la mise en œuvre des orientations nationales en matière de renforcement de l'utilisation des Systèmes d'information Nationales, le gouvernement tunisien a mis comme objectif, l'instauration d'un système d'identification unique du citoyen, ce projet est mené en collaboration entre l'état tunisien plus précisément le Centre Nationale de l'informatique (CNI) et LINAGORA.

Le ministère des TIC cherche, en effet, à ce qu'il y ait un ou quelques identifiants uniques pour chaque personne afin qu'elle puisse, justement, bénéficier des services offerts, à l'instar des soins dans les hôpitaux, du remboursement des médicaments, etc. Cet identifiant permettra également d'accélérer les procédures dans le traitement des dossiers à l'instar du paiement des impôts.

Les prestations objet de ce projet concerne notamment, la réalisation des actions globales suivantes :

- l'identification et l'authentification du citoyen
- Recenser tous les acteurs impliqués et leurs rôles détaillés dans le processus de délivrance de l'identifiant depuis sa naissance et durant son cycle de vie
- Les processus de collecte, de gestion, de mise à jour et des échanges des données se rapportant à l'identification du citoyen

- Recensement des services électroniques en exploitation, les identifiants utilisés, les mécanismes d'authentifications et les moyens de sécurités associés
- Réaliser un benchmarking international concernant les diverses politiques, choix et orientations gouvernementales dans les domaines de l'identification uniques du citoyen et la gestion des données y afférentes.
- Proposer les nouvelles orientations organisationnelles, légales, réglementaires et technologiques en matière d'identification unique du citoyen, notamment par rapport à l'adoption d'un identifiant national unique, ainsi qu'en matière de collecte, sauvegarde, gestion et échanges intersectoriels des données y afférentes

Ce projet est une première étape pour contribuer à un projet plus important relative à l'instauration d'une carte multi-services et multi-usage garantissant une identification et une authentification unique, forte et fiable du citoyen et permettant la centralisation de l'authentification en toute simplicité et sécurité aux différents services publics offerts.[N5]

1.4 Présentation de la mission du stage

Introduction

Mon stage se déroule dans le cadre du projet "mise en place d'un identifiant numérique unique pour chaque citoyen" et j'étais amené à intégrer le processus de travail des administrateurs système des deux équipes de LINAGORA et CNI.

Mission de stage

Mon travail consiste à concevoir le schéma d'annuaire, la conception de l'architecture globale de ce projet dans une première étape, dans une deuxième étape l'installation des services, la configurations des différents serveurs, la préparation et l'importation des données existantes dans l'annuaire, et finalement la migration des applications sur l'annuaire LDAP unifié.

Démarche du projet

- Conception du schéma LDAP
 - Recueil du besoin de l'état tunisien avec le CNI : types d'objets de l'annuaire (utilisateurs, groupes, applications,...)
 - Spécifications des objets de l'annuaire
 - Construction du schéma correspondant aux spécifications
- Conception de l'architecture LDAP (serveurs masters, slaves ...)

- Installation des services OpenLDAP
- Configuration de la synchronisation entre les masters et les slaves
- Installation de Linid Directory Manager
- Configuration de la délégation de gestion
 - Recueil du besoin avec le CNI : types de délégation
 - Spécifications de la délégation
 - Configuration et développements avancés
- Préparation des données et importation
- Pointage du WebSSO sur l'annuaire LDAP unifié
- Migration des applications sur l'annuaire LDAP unifié

1.5 Conclusion

Nous avons dans ce chapitre situé le projet dans son contexte spatial et temporel. Ceci, pour être en mesure dans le chapitre suivant pour introduire les concepts les plus importants qui y sont liés, afin d'aboutir à une étude théorique des notions principales de notre projet.

Chapitre 2

Concepts Clés

2.1 Introduction

Après avoir situer le projet dans son cadre général, nous consacrons ce chapitre pour notre étude théorique et la définition de quelques concepts clés .

2.2 LDAP

Definition d'un annuaire

Un annuaire électronique est un catalogue de données dont le but est de proposer, grâce à des fonctions de recherche, un accès rapide à ses ressources aux différents clients qui le consulte. Les annuaires électroniques permettent de créer, de modifier, d'effacer, de lister et d'organiser des données qu'ils contiennent.

Ils sont aussi des bases de données spécialisées. En effet, il existe un certains nombres de critères qui distingues les annuaires électroniques des bases de données conventionnelles.

Historique du Protocole

La forme des annuaires électroniques a bien évolué depuis leur apparition au début de l'ère informatique citons-en quelques uns :

- Unix : /etc/passwd (années 70-80)
- DNS (1984)
- X.500 (1988-1993-1997)
- LDAP (1993)
- **Standard X.500** : Ce standard a été conçu par des opérateurs de télécommunication , son objectif est de fédérer les annuaires de chaque opérateur et ainsi offrir un annuaire global. Parmi ses défauts est

l'obligation de s'appuyer sur une pile de protocoles OSI. Le protocole de base de X.500 s'appelle DAP (Directory Access Protocol ; protocole d'accès à l'annuaire)

- **Protocole LDAP**

LDAP est un protocole basé sur TCP/IP qui permet de partager des bases de données d'information sur un réseau interne (intranet) ou externe (internet). Ces bases de données sont appelées annuaire électronique, elles peuvent contenir tout type d'informations, des informations sur les personnes, à des données systèmes.

Le protocole LDAP est du type client serveur, le serveur contient la base de données, et le client consulte la base de données, le protocole fournit les bases pour cette communication entre la client et le serveur (normalisée par l'IETF[Ref] par la RFC2251), et les commandes nécessaires au client pour rechercher, créer, modifier ou effacer des données. LDAP est bien entendu sécurisé pour le transfert et l'accès aux données, avec des outils de cryptage comme SSL.

Par ailleurs LDAP fournit des outils pour que les serveurs d'annuaire puissent communiquer entre eux, on a ainsi la possibilité de créer des serveurs miroirs qui pourront se synchroniser, ou de relier simplement les serveurs entre eux. [N6]

Les models de LDAP

- **Le modèle d'information**

Le modèle d'information définit le type de données pouvant être stockées dans l'annuaire. L'élément de base est une entrée, et chaque entrée représente une instance d'une classe d'objet particulière qui contient des attributs avec chaque type d'attribut possède une syntaxe qui spécifie le format et l'encodage des valeurs des attributs associés à ce type.

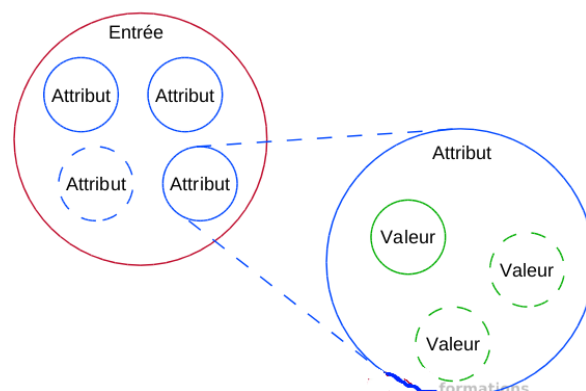


FIGURE 2.1 – Modèle d'information LDAP

Exemple des syntaxes les plus courantes :

- 1.3.6.1.4.1.1466.115.121.1.7 : Boolean
- 1.3.6.1.4.1.1466.115.121.1.12 : DN
- 1.3.6.1.4.1.1466.115.121.1.15 : Directory String (chaîne de caractères encodée en UTF-8)
- 1.3.6.1.4.1.1466.115.121.1.26 : IA5String (chaîne de caractères ASCII)
- 1.3.6.1.4.1.1466.115.121.1.27 : INTEGER (entier)

- Le modèle de nommage :

Le modèle de nommage définit comment sont organisées les entrées de l'annuaire et comment elles sont référencées. Les entrées sont stockées selon une structure logique hiérarchique appelée DIT (Directory Information Tree), au sein de cet arbre, les entrées sont identifiées par un nom, le DN (Distinguished Name) qui est unique dans l'annuaire et un RDN (Relative Distinguished Name) est unique dans sa branche.

C'est quoi le DIT ?

Le DIT est un outil de conception d'annuaire , il définit :

- Le contexte de nommage
- Les branches
- Les entrées des branches :
 - Leur RDN
 - Leurs classes d'objets

• Exemple de DIT

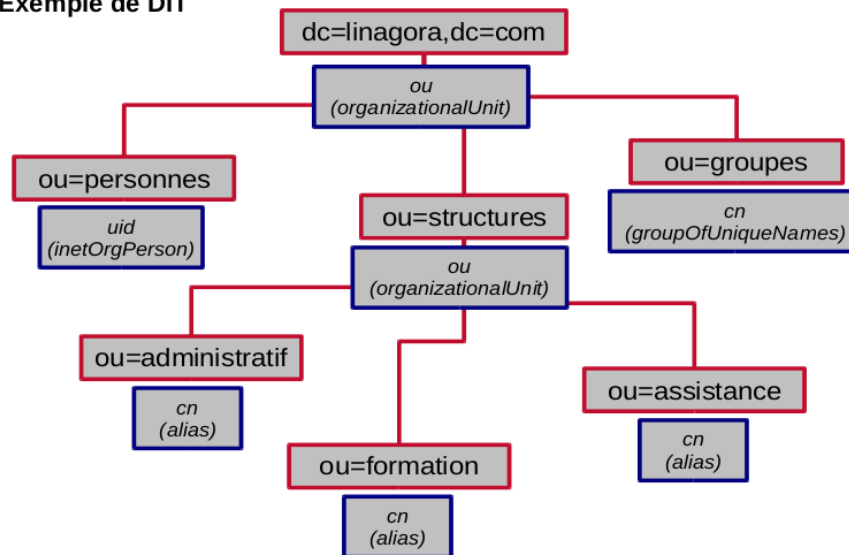


FIGURE 2.2 – Exemple de DIT

- **Le modèle fonctionnel**

Le modèle fonctionnel définit 9 opérations de base , trois types d'opérations se présentent :

L'accès au service

Pour l'accès au service on trouve 3 opérations de base

- Bind
 - S'authentifier auprès de l'annuaire.
 - Paramètres : DN et mot de passe (en clair).
 - Si pas de paramètres, la connexion est anonyme.
- Unbind
 - Se déconnecter auprès de l'annuaire.
 - Terminer la connexion TCP/IP.
 - Obligatoire pour mettre fin à une connexion.
- Abandon
 - Abandonne une opération asynchrone en cours
 - Paramètres : identifiant de l'opération

Mise à jour

Quatre opérations basiques se présentent :

- add
 - Ajout d'une nouvelle entrée.
 - Vérification par rapport au schéma.
 - Paramètres : totalité de l'entrée (DN + contenu).
- delete
 - Supprimer une entrée.
 - Paramètres : DN de l'entrée.
- modify
 - Modifier une entrée existante.
 - Vérification par rapport au schéma.
 - Plusieurs variantes possibles : add, delete, replace.
 - Paramètres : DN de l'entrée, variante, attribut et valeurs.
- modifyDN Principalement cette opération permet de Renommer une entrée

Interrogation

Deux opérations basiques se présentent :

- search
 - Effectuer une recherche
 - Seule opération pouvant obtenir plusieurs réponses
- compare
 - Exécuter un test d'égalité sur la valeur d'un attribut
 - Paramètres : DN, nom de l'attribut à tester, valeur à tester
 - Résultat = TRUE si l'entrée possède bien le couple attribut-valeur et FALSE si non.

- Le modèle de sécurité

Le modèle de sécurité décrit les moyens pour protéger les données de l'annuaire, La sécurité peut se faire à différents niveaux , soit lors de l'accès à l'annuaire, en nécessitant une authentification , soit lors de l'accès aux données, par des contrôles d'accès ou bien lors du transfert des données, par le chiffrement des flux qui permet d'assurer la confidentialité et l'intégrité des données

Que peut apporter LDAP ?

LDAP simplifie la gestion des profils de personnes et de ressources, favorise l'interopérabilité des systèmes d'informations à travers le partage de ces profils, et améliore la sécurité d'accès aux applications. De façon générale, un annuaire LDAP d'entreprise (groupware, intranets...) permet de réduire les coûts d'administration et d'améliorer la sécurité. Un annuaire LDAP pour les applications de e-business (commerce électronique, extranets...) permet de mieux gérer les profils des utilisateurs, de favoriser la personnalisation des services et de déléguer l'administration à des utilisateurs externes à l'entreprise tout en contrôlant la sécurité. [B1]

Différence entre une base de donnée et un annuaire

LDAP contient des classes d'objets qui définissent des personnes, des applications et des groupes, qui sont normalisés par l'IETF. On retrouve ces classes dans tous les outils conformes au standard LDAP.

Les majeurs différences entre une base de donnée et un annuaire :

- On lit plus souvent un annuaire qu'on le met à jour. Contrairement à un SGBD, un annuaire n'est pas fait pour stocker des informations constamment en mouvement. Il est logique de le structurer différemment et d'organiser les données de manière arborescente (sur un SGBD, la structuration est relationnelle).
- Un annuaire fournit une méthode de consultation standardisée. Le SQL est, certes, standardisé, mais chaque SGBD (Oracle, SQLServer, MySQL, PostgreSQL ...) a sa propre couche de connexion et ses propres fonctions.
- La norme LDAP définit le modèle de données, alors qu'un SGBD varie (quoi, où et comment). Avec les schémas, un annuaire fournit des modèles de données officialisés , ce qui permet d'être interopérable. [B2]

2.3 LSC : LDAP Synchronization Connector

Le logiciel LDAP Synchronization Connector est un moteur de synchronisation entre annuaires LDAP, bases de données, fichiers, et autres sources (API REST, etc.). Il est particulièrement efficace pour diffuser les données d'utilisateurs et de groupes entre son annuaire d'entreprise, un serveur OpenLdap et une base de données d'application. On peut le classer dans la catégorie des logiciels de Méta-annuaire ou de gestionnaire d'identités.

2.4 WebSSO [Single-Sign-On]

Definition

SSO signifie «Single Sign On», qui peut se traduire en français par « authentication unique » . L'objectif d'une architecture informatique SSO est qu'un utilisateur s'authentifie une première fois pour ouvrir sa session de travail et accède ensuite à toutes ses applications sans rentrer de nouveau son (ou ses) mot(s) de passe.

Le SSO regroupe donc plusieurs fonctionnalités :

- Couple identifiant/mot de passe unique
- Transmission transparente des informations de session aux applications
- Gestion des profils applicatifs, c'est-à-dire qui accède à quoi

Le SSO n'empêche pas un utilisateur d'avoir plusieurs couples identifiant/mot de passe, seulement il n'en utilise qu'un pour s'authentifier, les autres sont liés par session et communiqués aux applications.

Modes du SSO

- SSO par agent :
Un agent est installé sur le poste client, c'est l'agent qui intercepte les flux des applications et pousse les mots de passe. Ce mode est utilisé généralement pour les clients lourds, pas pour le WebSSO

SSO par agent

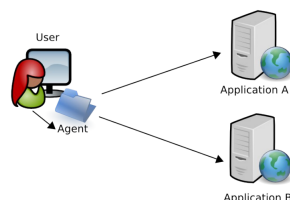


FIGURE 2.3 – SSO par agent

- SSO par délégation :
Un agent est installé sur le serveur d'application, cet agent intercepte les requêtes à destination de l'application, et redirige l'utilisateur sur le portail si ce dernier n'a pas de session SSO active

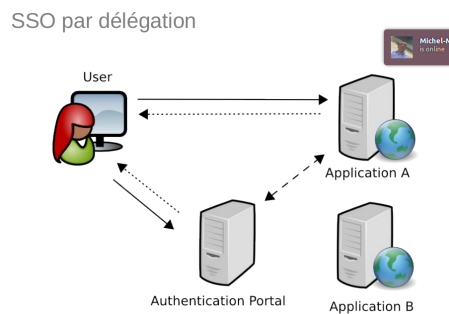


FIGURE 2.4 – SSO par délégation

- SSO par mandataire inverse (reverse-proxy) :
Le serveur d'application n'est pas accédé directement par les utilisateurs, mais seulement par le portail WebSSO, c'est l'agent qui intercepte les flux des applications et pousse les mots de passe donc c'est le portail qui vérifie la session SSO de l'utilisateur et qui joue ensuite le rôle de mandataire entre l'utilisateur et l'application

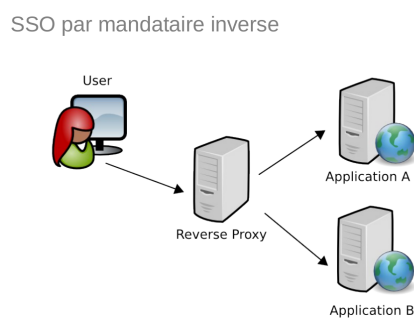


FIGURE 2.5 – SSO par mandataire inverse (reverse-proxy)

2.5 Protocole HTTP

Présentation

HTTP signifie « HyperText Transfer Protocol ». La version 1.0 date de 1996, la version 1.1 (actuelle) de 1997. Le protocole définit les échanges entre un client HTTP qui est le navigateur web et un serveur HTTP, le serveur délivre au client des ressources identifiées par une URL ReF (« Uniform Resource Locator »)

HTTP - Requête

Une requête HTTP se découpe en :

- une ligne de requête, comprenant trois champs séparés par des espaces :
 - la méthode (GET, HEAD, POST, PUT, DELETE, ...)
 - URL
 - la version HTTP (HTTP/1.0, HTTP/1.1, ...)
- des lignes d'en-têtes (headers), avec un couple attribut : valeur » par ligne (attributs courants : User-Agent, Accept-Encoding, ...).
- une ligne vide.
- le corps de la requête, généralement vide mais pouvant contenir les attributs et les valeurs d'un formulaire utilisant la méthode POST.

HTTP - Réponse

Une réponse HTTP se découpe en :

- une ligne de statut, comprenant trois champs séparés par des espaces :
 - la version HTTP (HTTP/1.0, HTTP/1.1, ...)
 - le code de réponse (200, 403, 404, ...)
 - le message de réponse (OK, FORBIDDEN, NOT FOUND, ...)
- des lignes d'en-têtes (headers), avec un couple « attribut : valeur » par ligne (attributs courants : Location, Content-Type, ...)
- une ligne blanche
- le corps de la réponse, qui contient le document demandé

HTTP - Cookie

Le protocole HTTP est dit « sans état » (stateless) car d'une requête à l'autre, aucune information de connexion n'est conservée. Le problème peut être contourné :

- connexions persistantes en HTTP 1.1 (Keep-Alive)
- sessions côté serveur
- cookies côté client

Les cookies sont des fichiers textes de 4096 octets maximum stockés

sur le disque dur du client, un cookie possède (un nom ,une valeur, un domaine ou un hôte, un chemin et des options)

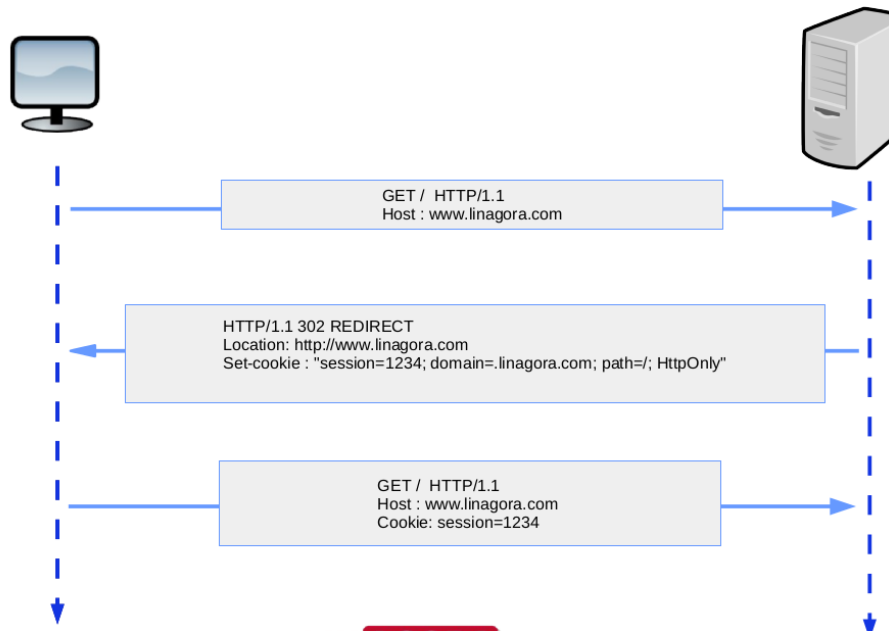


FIGURE 2.6 – HTTP – Création d'un cookie

2.6 Conclusion

A travers ce chapitre, nous avons présenté une étude théorique des notions principales à notre projet , afin d'approfondir nos connaissances sur le fondement théorique des annuaires. Une étude de Ldap et du WebSSO, nous a permis d'avoir une vue d'ensemble sur les fonctionnalités fondamentales de notre projet. Cette vue globale est le pilier et le support des besoins rédigés dans le cahier des charges que nous exposerons dans le chapitre suivant.

Chapitre 3

Spécifications des besoins

3.1 Introduction

Durant ce chapitre, nous allons décrire une vue claire des différents besoins escomptés de notre travail. Pour ce faire, nous fournirons, tout d'abord, une analyse approfondie du problème, afin de dégager un ensemble de besoins fonctionnels et non fonctionnels auxquels notre travail doit répondre. Ensuite, nous définirons les différents acteurs qui seront mis en jeu, ainsi que quelques diagrammes de cas d'utilisation selon le formalisme UML.

3.2 Analyse des besoins

Dans cette section, nous précisons les objectifs principaux de ce projet et nous préciserons à la fois les exigences fonctionnelles et non fonctionnelles qui doivent être remplies pour les atteindre.

Les objectifs du projet

L'objectif global de ce projet est la mise en place d'un annuaire de l'état tunisien dans le cadre de l'obtention de chaque citoyen d'un identifiant unique qui sera utilisé plus tard pour l'authentification aux applications nationales qui seront intégrées dans l'intranet des ministères via le WebSSO.

Besoins fonctionnels

Un besoin fonctionnel exprime une action qu'un système doit être capable d'effectuer en réponse à une demande. Il décrit les sorties qui sont produites pour un ensemble donné d'entrées. Notre Systeme est amenée à couvrir un ensemble de besoins. Un bref descriptif est donné dans ce qui suit :

Besoins non fonctionnels

Les exigences non fonctionnels du projet sont :

- **Disponibilité** : Le système doit fonctionner sans arrêt
- **Scalabilité** : Le système doit prendre en charge l'évolutivité d'au moins 60 de la charge maximale.
- **Sécurité** : Le système doit assurer un niveau élevé de sécurité
- **Performance** : Le système doit assurer des milliers de requêtes instantanées de recherche d'employées ou de structures

3.3 Vue fonctionnelle du système

Après l'analyse et l'identification des exigences fonctionnelles et non fonctionnelles, ces données sont agrégées pour décrire clairement ces besoins à travers les diagrammes suivants qui illustrent les scénarios détaillés des différentes interactions.

Identification des acteurs

L'acteur est un élément externe qui interagit avec le système, il prend des décisions et des initiatives. Dans notre cas nous pouvons définir les acteurs suivants :

- **Administrateur central** :

A le rôle de gérer les administrateurs « Principaux » (vis à vis) du premier niveau de la hiérarchie c'est-à-dire les administrateurs de chaque ministère. En plus l'administrateur central a le rôle de gérer les nouvelles catégories, fonctions, grades, secteurs d'activités, positions et types.

- **Administrateur Principal** :

A le droit de créer les responsables (employé ou structure) dans la structure à laquelle il appartient ainsi de créer des administrateurs « principaux » pour administrer les structures de plus bas niveau dans la hiérarchie. Par défaut chaque administrateur principal a le droit de gérer les employés et les sous structures de la structure à laquelle il appartient ou il délègue ce rôle à un autre.

- **Responsable structure** :

A des droits sur la structure à laquelle il est affecté et ses sous structures, il peut : consulter, ajouter, mettre à jour, valider la saisie par le responsable « structure » délégué et supprimer les sous structures. En plus il peut désigner le responsable « structure » délégué et lui affecter les rôles appropriés

- **Responsable employé :**

A des droits sur les structures et les sous structures que lui appartiennent, il peut : consulter, ajouter, mettre à jour, valider la saisie par le responsable « employé » délégué, et déplacer des employés. En plus il peut désigner le responsable « employé » délégué et lui affecter les rôles appropriés.

- **Employé :**

A des droits restreints tel que recherche des employés et structure ainsi que la navigation en plus la possibilité de modifier quelques informations qui lui concernent.

- **Citoyen :**

A seulement le droit de naviguer dans le service annuaire ainsi que la recherche d'une structure ou un employé.

Cas d'utilisation global

La figure ci-dessous présente le cas d'utilisation global

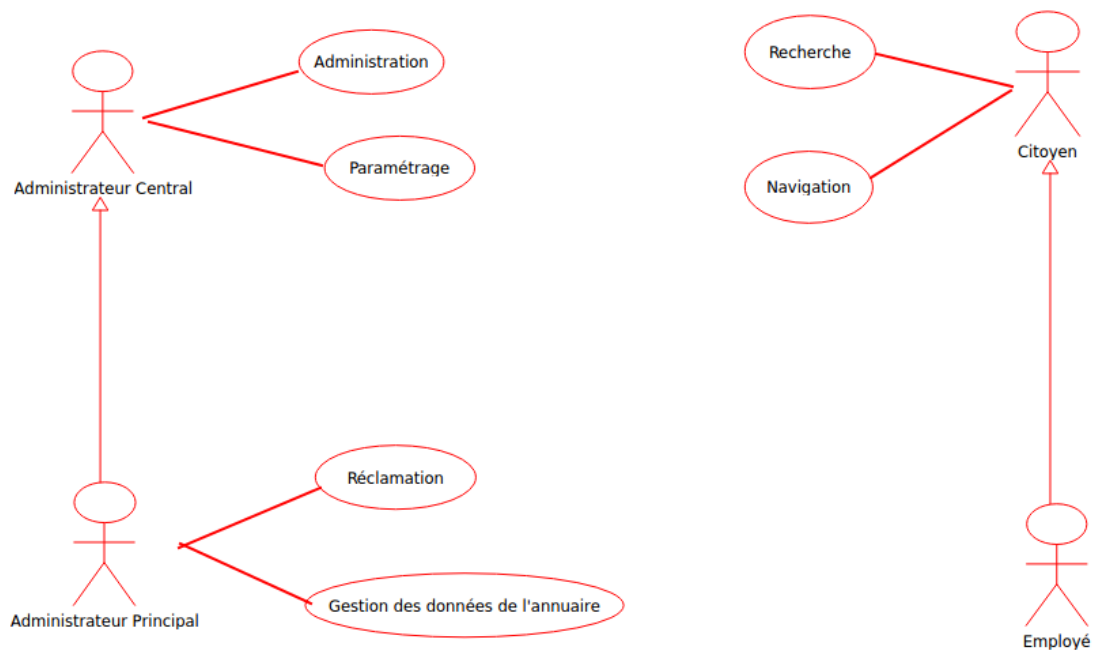


FIGURE 3.1 – Diagramme de cas d'utilisation globale

Raffinement du cas d'utilisation « Recherche »

La figure ci-dessous présente le raffinement du cas d'utilisation Recherche

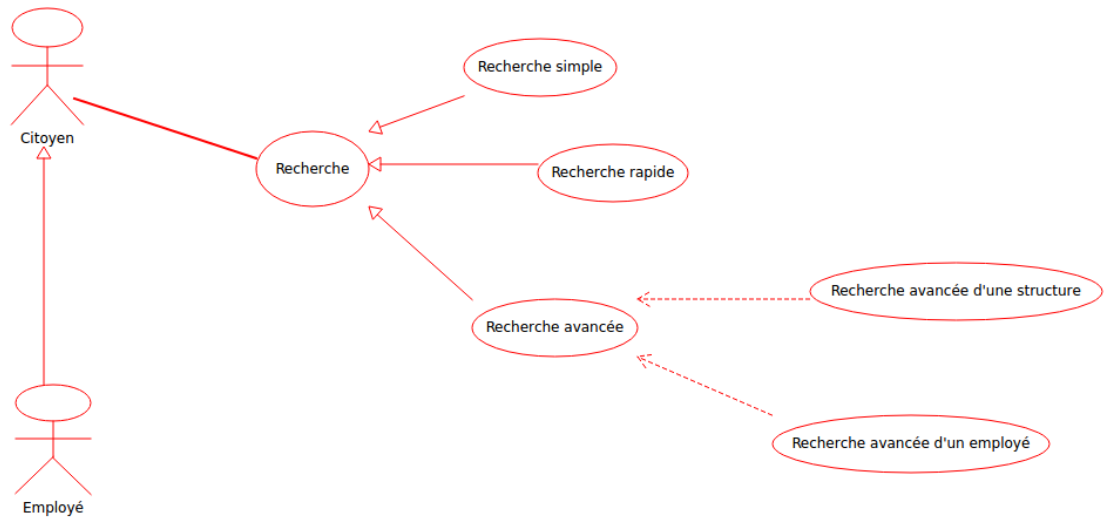


FIGURE 3.2 – Diagramme de Raffinement de cas d'utilisation « Recherche »

Cas d'utilisation « Recherche avancée »

Nous allons détailler ce cas d'utilisation nommé recherche avancée

Nom : Recherche avancée

Acteur : Citoyen

Description : une recherche avancée consiste à définir plus d'information dans le formulaire de recherche pour trouver une structure ou un employé dans l'administration tunisienne.

Pré condition : L'utilisateur doit accéder au service annuaire

Démarrage : l'utilisateur a demandé la page de recherche avancée.

Scénario nominal :

- Le système affiche le formulaire de recherche avancée.
- L'utilisateur sélectionne s'il va chercher un employé ou une structure de l'administration tunisienne.
- Le système vérifie le choix de l'utilisateur (employé ou structure), s'il va chercher un employé le système fait appel au cas d'utilisation « recherche avancée employé » si non le système fait appel au cas d'utilisation « recherche avancée structure ».

- Le système affiche le résultat de recherche.

Diagramme de sequence système de cas d'utilisation « recherche avancée employé »

La figure suivante présente le diagramme séquence de l'opération de recherche avancée. Le citoyen est l'acteur de cette tâche.

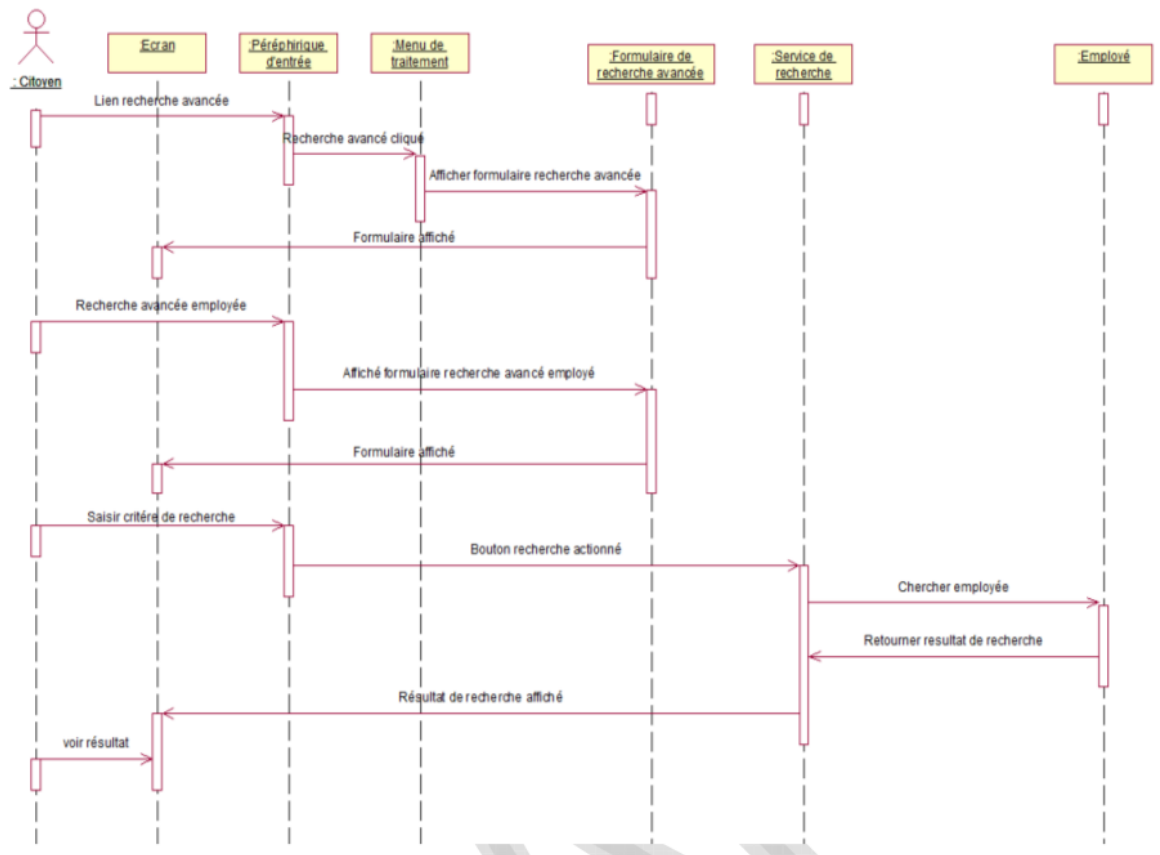


FIGURE 3.3 – Diagramme de sequence de cas d'utilisation « Recherche avancée employé »

Description textuelle « Recherche avancée employé ».

- L'utilisateur sélectionne un type recherche employé.
- LinID affiche le formulaire de recherche.
- L'utilisateur introduit les données pour chercher un employé.

- La recherche employé se lance.
- Le control recherche récupère le résultat à partir de l'annuaire et charge LinID pour afficher le résultat de recherche.
- LinID affiche le résultat de recherche.

Raffinement du cas d'utilisation « Navigation »

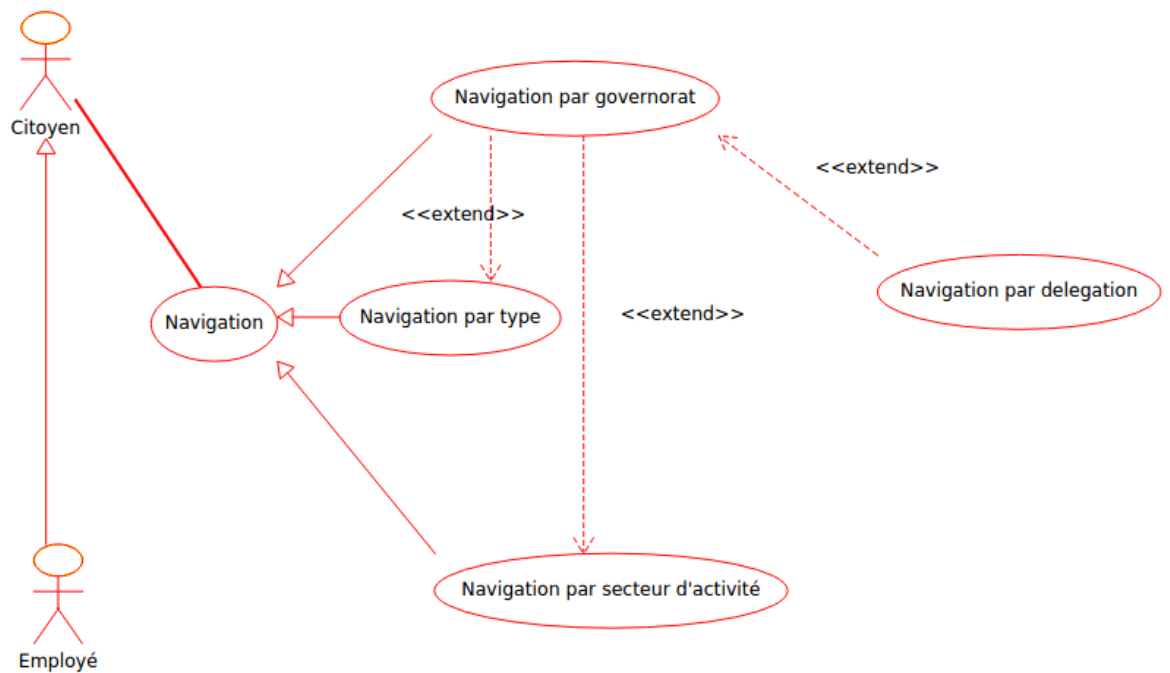


FIGURE 3.4 – Diagramme de Raffinement de cas d'utilisation «Navigation»

Cas d'utilisation : Navigation par type

Nous allons détaillé par la suite un cas d'utilisation « Navigation par type »

Nom : Navigation par type

Acteur : Citoyen

Description : la navigation par type consiste à charger et afficher des pages suite à des cliques sur des liens bien précis pour afficher à la fin les informations détaillées concernant un employé ou une structure.

Pré condition : L'utilisateur doit accéder au service annuaire

Démarrage : L'utilisateur accède à l'annuaire

Scénario nominal :

- Le système affiche la liste de type structure.
- L'utilisateur choisit et clique sur l'un des types affichés.
- Le système affiche la liste des structures qui appartient à ce type regroupé par gouvernorat.
- L'utilisateur choisit et clique sur un gouvernorat parmi la liste affichée.
- Le système affiche la liste des structures qui ont le type déjà choisi et appartenant au gouvernorat sélectionné, qui sont regroupé par délégation (les délégations appartenant au gouvernorat sélectionné).
- L'utilisateur choisit une structure parmi la liste des structures groupées par délégation.

Scénario alternatif :

L'utilisateur décide de sélectionner une structure parmi la liste affichée.

Scénario exceptionnel :

Le système affiche une liste vide.

**Diagramme de sequence système de cas d'utilisation
« Navigation par type » :**

La figure suivante présente le diagramme de séquence de l'opération de navigation par type. L'acteur de cette tâche c'est le citoyen.

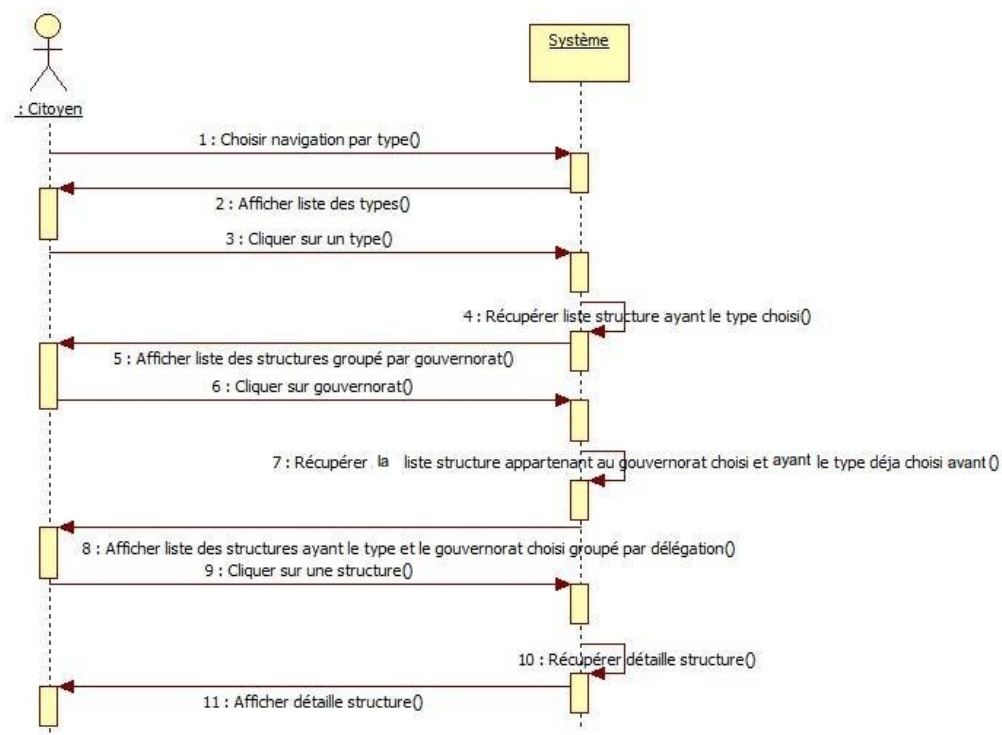


FIGURE 3.5 – Diagramme de sequence système de cas d'utilisation « Navigation par type »

Diagramme de Collaboration de cas d'utilisation « Navigation par type »

La figure suivante présente le diagramme de collaboration de l'opération de navigation par type, et l'acteur de cette tâche c'est le citoyen.

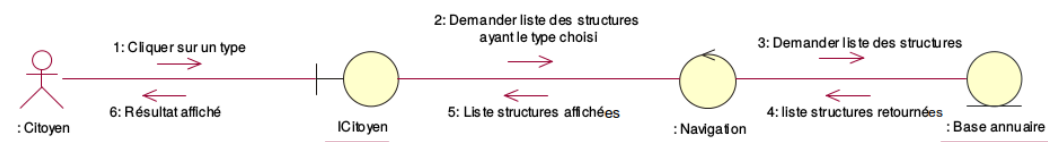


FIGURE 3.6 – Diagramme de Collaboration de cas d'utilisation « Navigation par type »

Présentation textuelle des flots d'événement :

Dans ce contexte la description textuelle suivante n'est autre que le flot d'événement qui vient de compléter le diagramme de collaboration montré précédemment.

- Le Citoyen clique sur l'un des types affichés sur l'écran.
- LinID envoie le type sélectionné pour récupérer les structures correspondante.
- Le Control envoie le critère à l'annuaire.
- LinID Récupère les structures ayant le type choisit.
- LinID affiche le résultat de recherche.

3.4 Vue technique du système

La capture des besoins techniques est une activité primordiale pour la phase de conception architecturale. Dans cette partie, nous allons étudier le système de point de vue technique à travers la conception du schéma de l'annuaire avec la spécification de l'architecture adopté pour le système.

Spécification des Besoins techniques

Après avoir détailler dans la partie précédente les besoins fonctionnels de notre projet, nous penchons maintenant sur les besoins opérationnels que doit fournir notre système. L'implémentation de ces besoins, dits non fonctionnels, se fait tout au long du cycle de vie du produit.

Sécurité

Nous devons conférer une ample importance à la sécurité. Afin d'accéder à la consultation de l'interface LinID , l'utilisateur doit s'authentifier par un login et password unique , qui sont d'ailleurs indiqués dans l'annuaire construit avec un login unique (numéro de CNRPS) et un mot de passe spécifique pour chaque utilisateur (administrateur, employé ou citoyen).

Performance

Le système doit être disponible et opérationnelle à tout moment, et il doit assurer un fonctionnement fiable, nous expliquerons dans le chapitre suivant comment assurer la performance de notre système.

Extensibilité

Il faut tenir compte de la possibilité de l'extension du système, de la réalisation des modifications et de sa portabilité.

Spécification de l'annuaire centralisé

Le but de cette section est de spécifier les besoins d'un point de vue technique et fonctionnel pour le projet de gestion centralisée des identités. Les composants entrant en action sont :

- un annuaire LDAP.
- une interface d'administration d'annuaire [LinID].
- des connecteurs de synchronisation.

Annuaire LDAP

L'annuaire reposera sur l'implémentation OpenLDAP. Il sera alimenté par différentes sources, et proposera quelques attributs supplémentaires pour lequel il sera le référentiel maître.

Interface d'administration d'annuaire

L'interface d'administration de l'annuaire est faite avec la suite logicielle LinID qui est la seule suite logicielle de gestion d'identités complète Open Source, qui permet au clients de gagner en efficacité et en sécurité dans la gestion des données d'identité, d'accès et d'habilitation.

Connecteurs de synchronisation

Les connecteurs de synchronisation sont principalement gérés par le LSC qui est un moteur de synchronisation entre annuaires LDAP, bases de données, fichiers, et autres sources.

3.5 Conclusion

A travers ce chapitre, nous avons présenté les besoins et les exigences des différentes fonctionnalités, ainsi que les relations qui devront prendre place séquentiellement. Nous avons, ainsi présente les spécifications de l'annuaire centralisé, ce qui nous permettra d'aborder la prochaine étape, à savoir la phase de conception de l'annuaire ainsi l'architecture réseau dont nous avons implémenté la solution.

Chapitre 4

Conception de l’annuaire et Architecture

4.1 Introduction

Ce chapitre sera consacré à la conception de l’annuaire et à la présentation de l’architecture réseau proposé suivie lors de l’implémentation.

4.2 Annuaire LDAP

Dans cette phase, nous allons présenter la structure d’annuaire (DIT) et le schéma d’annuaire.

Structure d’annuaire

La structure arborescente de l’annuaire est définie comme suit :

- la branche « ou=users » comprendra tous les utilisateurs à plat.
- la branche « ou=groups » contiendra les groupes statiques et dynamiques, à plat.
- la branche « ou=infrastructure » contiendra les comptes techniques, les groupes techniques, et les éléments indispensables au fonctionnement du SSO (configuration, sessions, sessions persistantes).
- la branche « ou=structures » comprendra toutes les structures organisées de manière arborescente.
- la branche « ou=ppolicy » comprendra l’unique politique de mots de passe appliquée à toutes les entrées.
- La branche « ou=nomenclature » comprendra toutes les nomenclatures nécessaires.

- La branche « ou=applications » permet de gérer les accès aux applications.

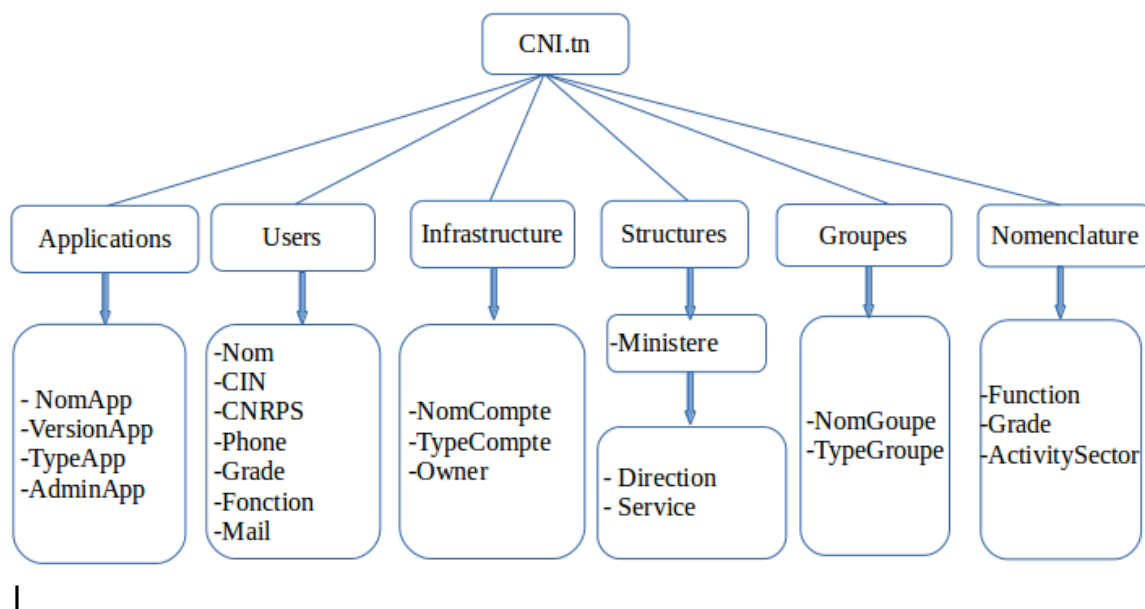


FIGURE 4.1 – Structure d’annuaire

C’est l’organigramme globale de notre annuaire, avec la branche structure qui est la plus compliquée, vue que le centre national de l’informatique administre des différents ministères, donc la structure va différer d’un ministère à un autre. Nous donnerons par la suite un exemple de structure d’un ministère.

Schéma d’annuaire

Dans cette section on va détailler les deux branches les plus importantes et plus délicates pour ce projet , que sont [Personnes, Structures]. Ces deux branches doivent être écrites dans un fichier qu’on peut nommer CNI.schema dont nous indiquerons les classes d’objet et les attributs de chacune.

Personne

La nature d’une Personne dans le référentiel LDAP est définie dans le tableau ci-après :

Nom de l'attribut	Description	Type d'attribut	Obligatoire ?
objectClass	Nature de l'objet LDAP Valeur en dur : top ; person ; organizationalPerson ; inetOrgPerson ; linidPeople ; govPerson	Liste de classes d'objets	oui
idAgent	Identifiant unique de l'agent : numéro de tiers (matricule CNRPS)	Chaîne de caractères	oui
sn ; fr	Nom de l'agent en Français	Chaîne de caractères	oui
cn ; fr	« Prénom [espace] Nom » de l'agent en Français	Chaîne de caractères	oui
givenName ; fr	Prénom de l'agent en Français	Chaîne de caractères	oui
sn ; ar	Nom de l'agent en Arabe	Chaîne de caractères	oui
cn ; ar	« Prénom [espace] Nom » de l'agent en Arabe	Chaîne de caractères	oui
givenName ; ar	Prénom de l'agent en Arabe	Chaîne de caractères	oui
govCIN	Numéro de Carte d'identité nationale de la personne	entier	non
personalTitle	Civilité de l'agent (M., Mlle, Mme)	Chaîne de caractères	non
govCNSS	Numéro de la Caisse nationale de sécurité sociale de la personne	entier	non
govFunction	la fonction du citoyen	Chaîne de caractères	oui
govFunction-StartDate	la date d'obtention du grade par l'employé	Chaîne de caractères	non
govDegree	la grade de l'employé	Chaîne de caractères	oui
govDegree-StartDate	la grade de l'employé	Chaîne de caractères	non
govBirthdate	date de naissance du citoyen	Chaîne de caractères	non
govFatherFirstName	le nom du grand pere	Chaîne de caractères	non
govGrandFather-FirstName	le prénom du grand père	Chaîne de caractères	non
govMotherFirstName	le prénom de la mère	Chaîne de caractères	non

TABLE 4.1 – Spécification de l'objet de classe Personne

Structure

Les structures sont l'organisation hiérarchique du CNI. les structures sont différentes d'un ministère à un autre , nous donnons l'exemple de la structure du ministère de finance dans l'annexe ajouté avec ce rapport.

Nom de l'attribut	Description	Type d'attribut	Obligatoire
objectClass	Nature de l'objet LDAP (une structure) Valeur en dur : top ;organizationalUnit ; linidStructure	Liste de classes d'objets	oui
ou	Nom de la structure	Chaîne de caractères	oui
description	Description de la structure	Chaîne de caractères	non
govStructuretype	Type de la structure , Valeurs possibles : - Direction Generale - Direction Regionale - Sous Direction - Unité - Cabinet	Chaîne de caractères	oui
postalAddress	l'adresse postale de la structure	Chaîne de caractères	oui
telephoneNumber	le numéro de téléphone fixe de la structure	Chaîne de caractères	oui
govActivitySector	le secteur d'activité d'une structure	Chaîne de caractères	oui
governorate	le gouvernorat dans lequel se situe la structure	Chaîne de caractères	oui
mail	l'adresse mail de la structure	chaîne de caractères	non
govContact	le contact de la structure	Chaîne de caractères	non
govWebsite	le réseau social de la structure	entier	non

TABLE 4.2 – Spécification de l'objet de classe Structure

Groupes

En parallèle des structures, les groupes correspondants sont créés. Deux types de groupes se présentent : groupes statiques et groupes dynamiques, leur nature est définie ci-après :

- **Groupes dynamiques :**

Nom de l'attribut	Description	Type d'attribut	Obligatoire
objectClass	Nature de l'objet LDAP (un groupe dynamique) Valeur en dur : top;groupOfURLs;linidDynamicGroup;cniDynamicGroup	Liste de classes d'objets	oui
cn	Nom du groupe dynamique	Chaîne de caractères	oui
memberURL	Requête LDAP de récupération automatique des membres de la structure et de toutes ses sous-structures	Chaîne de caractères	non
member	Membres de la structure et de toutes ses sous-structures (attribut rempli automatiquement par l'exécution de memberURL)	DN	non
cniMemberURL	Requête LDAP de récupération automatique des membres de la structure	Chaîne de caractères	non
cniDynamicMember	Membres de la structure (attribut rempli automatiquement par l'exécution de cniMemberURL)	DN	non
cniStaticMember	Pointeur vers les groupes dynamiques correspondant aux structures filles	DN	non

TABLE 4.3 – Spécification de l'objet groupe dynamique

- **Groupe statiques**

En plus des groupes dynamiques, des groupes statiques peuvent être créés. Leur nature est définie ci-après :

Nom de l'attribut	Description	Type d'attribut	Obligatoire
objectClass	Nature de l'objet LDAP (un groupe statique) Valeur en dur : top ;groupOfNames ; linid-StaticGroup	Liste de classes d'objets	oui
cn	Nom du groupe	Chaîne de caractères	oui
member	Membre du groupe (autres groupes ou utilisateurs)	DN	oui
description	Description du groupe	Chaîne de caractères	non

TABLE 4.4 – Spécification de l'objet groupe statique

Applications et rôles applicatifs

Des rôles applicatifs pourront être déterminés par application. Une application sera définie par les attributs suivants :

Nom de l'attribut	Description	Type d'attribut	Obligatoire
objectClass	Nature de l'objet LDAP (une application) Valeur en dur : top ;organizationalUnit ; linidApplication	Liste de classes d'objets	oui
ou	Nom de l'application	Chaîne de caractères	oui
description	Description de l'application	Chaîne de caractères	non

TABLE 4.5 – Spécification de l'objet Applications

Les rôles seront stockés sous les applications et contiendront une liste d'agents, comme défini dans le tableau suivant :

Nom de l'attribut	Description	Type d'attribut	Obligatoire
objectClass	Nature de l'objet LDAP (un rôle) Valeur en dur : top ;groupOfNames ; lini-dRole	Liste de classes d'objets	oui
cn	Nom du rôle	Chaîne de caractères	oui
member	Membre du rôle (autres rôles ou utilisateurs)	DN	oui
description	Description du rôle	Chaîne de caractères	non
memberOf	Rôle dont ce rôle est membre	DN	non

TABLE 4.6 – Spécification de l'objet Rôles applicatifs

Extensions activées

Les extensions suivantes seront activées :

- la politique des mots de passe (ppolicy), de manière basique pour s'accorder avec la politique d'administration
- le calcul inverse de groupes (memberOf)
- l'intégrité référentielle (refint), pour conserver l'intégrité sur les membres de groupes supprimés. En outre, l'annuaire sera indexé et optimisé par rapport à sa volumétrie, son schéma, et sa structure. (DIT)

4.3 Architecture de la solution

Dans cette phase nous présenterons l'architecture réseau globale qui assure la communication et le transport de flux entre les différents structure de l'état tunisien, ainsi la solution de l'architecture que nous avons présenté afin d'assurer le bon fonctionnement du système.

Architecture réseaux globale

La figure ci-dessous montre les relations entre le cœur du réseau et les différents établissements de l'état Tunisien , elle est divisée en cinq couches : [**Réseaux distants, Couche Edge fournisseurs, Couche Edge, Couche Core, Couche Agrégation**].

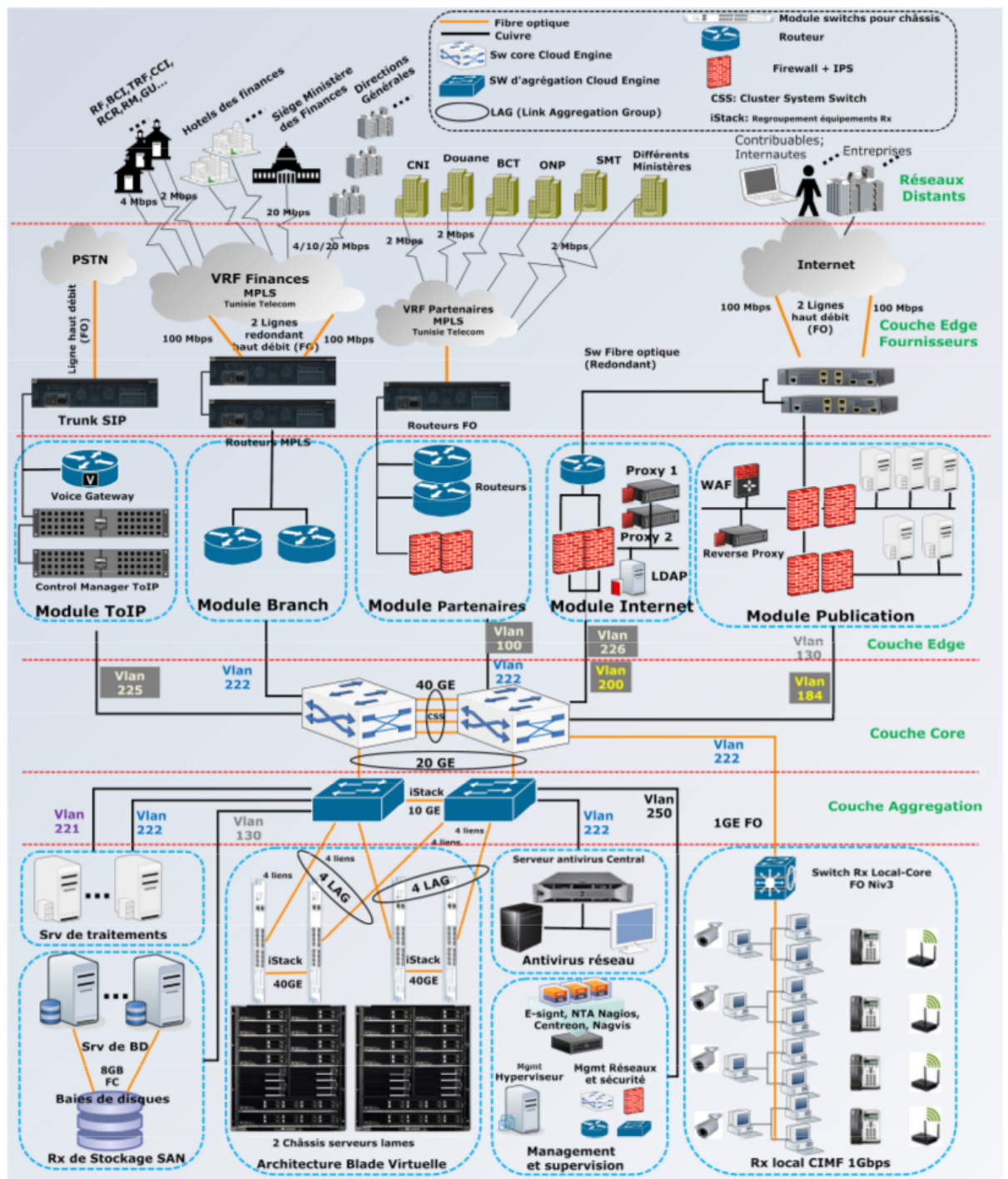


FIGURE 4.2 – Architecture réseau globale

Nous nous intéresserons par la suite de la couche Edge plus précisément par le module Internet dont nous avons implémenter la solution.

La figure ci-dessous présente l'architecture que nous avons proposé pour implémenter l'annuaire ainsi le WebSSO.

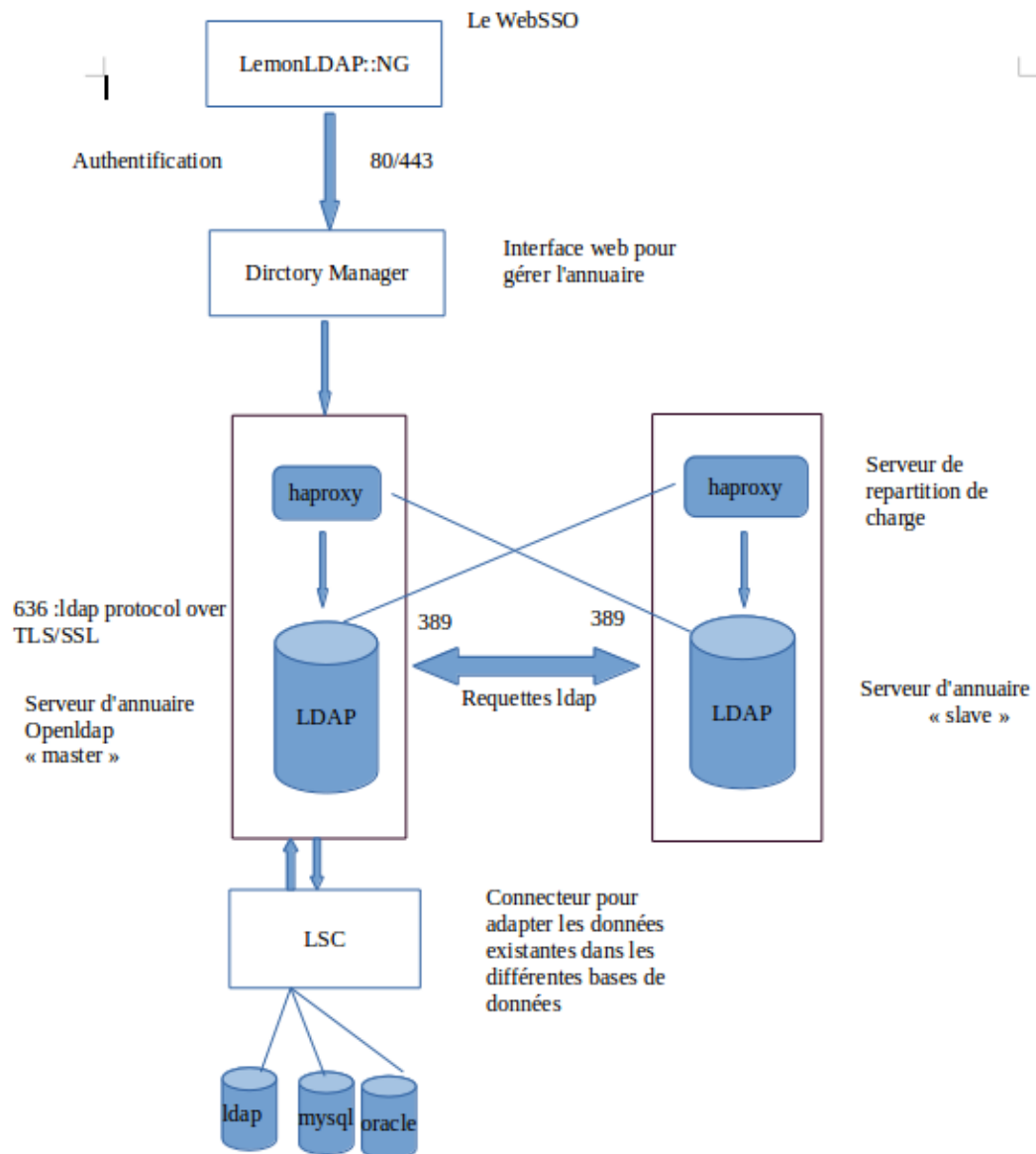


FIGURE 4.3 – Specification Couche EDGE

Cette architecture comporte les serveurs que nous avons utilisé durant la réalisation de ce projet. Nous avons utilisé deux serveurs physiques pour installer deux serveurs d'annuaire répliqués afin d'assurer la haute disponibilité, le premier serait master et l'autre serait slave. Un utilisateur se connecte au portail du CNI , il s'authentifie avec son uid qui est le numéro de CNRPS ou son mail en saisissant son mot de passe, une redirection se fait vers l'interface web de l'annuaire (**LinID**) pour faire les opérations souhaitées, qui de son tour communique avec le serveur d'annuaire pour extraire les données et les afficher. Le connecteur LSC est utilisé par les administrateurs pour extraire et adapter les données des différentes source vers l'annuaire.

Conclusion

Dans ce chapitre nous avons effectué une conception détaillé de l'annuaire ainsi nous avons montré l'architecture de l'annuaire .Nous passons maintenant au chapitre suivant, là où nous allons exposer la réalisation et le déploiement de l'annuaire.

Chapitre 5

Réalisation du Projet

5.1 Introduction

DANS ce dernier chapitre, nous allons présenter l'environnement de travail matériel et logiciel mis en place, ainsi nous présenterons les différentes étapes de la réalisation du projet accompagnées par des imprimés écrans.

5.2 Environnement de travail

Au cours de ce stage, et afin de réaliser notre projet, un ensemble de technologies et d'outils de travail ont été utilisés.

Environnement matériel

Pendant la réalisation du projet, nous avons eu besoins d'une machine et des serveurs ayant les caractéristiques suivantes :

- Ordinateur portable personnel
 - Marque d'ordinateur : LENOVO G50
 - Type de microprocesseur : Intel core i5 2.40GZ
 - Systeme d'exploitation : Ubuntu 14.04 TLS
 - Capacité de la RAM : 16 GO
 - Capacité du du disque dur : 1 TB
- Serveur 1 et 2 :
les deux serveurs sont similaires.
 - > Dimensionnement
 - CPU : 2 cœurs 4Ghz 64 bits
 - Systeme d'exploitation : Centos 7
 - Capacité de la RAM : 32 GO

Environnement logiciel

Après avoir présenter l'environnement matériel , nous rappellerons les choix techniques que nous avons choisis en les répartissant selon l'environnement :

OpenLDAP

Service d'annuaire qui permet de centraliser des informations telles que : les informations sur les utilisateurs (nom, prénom...), les données d'authentification pour les utilisateurs, les structures, les ressources, les droits d'accès.



FIGURE 5.1 – OpenLDAP

Latex

Est un système de composition de documents créé par Leslie Lamport en 19831. Plus exactement, il s'agit d'une collection de macro-commandes destinées à faciliter l'utilisation du « processeur de texte ». Il est particulièrement utilisé dans les domaines techniques et scientifiques pour la production de documents de taille moyenne ou importante. [REF 19]

Umbrello

Umbrello est un projet issu de sourceforge et déposé sous licence GNU GPL , Sans aucuns complexes, Umbrello a pour but de proposer à la communauté GNU/Linux un outil permettant la modélisation UML et la génération de code. Bien entendu, loin du ténor Together, il semble utile de préciser que cet outil n'a pas la prétention apparente de concurrencer les outils commerciaux en proposant une alternative "libre".

Ne proposant pas la plétore de modules d'un Together, on appreciera Umbrello du fait de sa simplicité d'utilisation, du respect de la notation UML, de son interface rapide et intuitive. On est en effet loin des outils réalisés en Java comme Together ou Poseidon for UML, qui peinent dès lors qu'il n'y a pas assez de RAM.

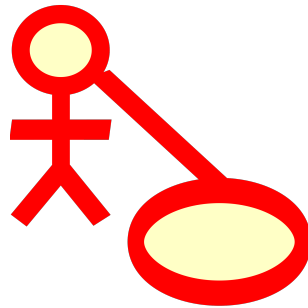


FIGURE 5.2 – Umbrello

Apache Directory Studio

Apache Directory Studio est une plateforme complète d'outillage destiné à être utilisé avec un serveur LDAP. C'est une application Eclipse RCP, composé de plusieurs plugins Eclipse (OSGi), qui peuvent être facilement mis à niveau avec les autres.



FIGURE 5.3 – Apache Directory Studio

Apache Web Server

Apache est un serveur web qui permet à des clients d'accéder à des pages web, c'est-à-dire en réalité des fichiers au format HTML à partir d'un navigateur installé sur leur ordinateur distant. Un serveur web est donc un « simple » logiciel capable d'interpréter les requêtes HTTP arrivant sur le port associé au protocole HTTP (par défaut le port 80), et de fournir une réponse avec ce même protocole.



FIGURE 5.4 – Appache Web Server

5.3 Taches réalisées

Nous commencerons par présenter les tâches faites durant la réalisation de ce projet que nous pouvons le diviser en deux parties , la première est l'implémentation de l'annuaire qui est la tache principale et la deuxième, est l'installation d'une application qui est la solution web mail de LINAGORA en l'intégrant avec l'annuaire et le Websso , qui est la tache secondaire.

Implémentation et configuration du serveur d'annuaire

La configuration de OpenLDAP se fait en plusieurs étapes :

- **Configuration du fichier slapd.conf**

Dans le fichier slapd.conf nous commençons par indiquer les cordonnées du rootdn qui va pouvoir s'authentifier en tant que administrateur pour modifier le schéma d'annuaire.

```
database      hdb
suffix        "dc=cni,dc=tn"
rootdn       | "cn=Manager,dc=cni,dc=tn"
rootpw       | secret
directory    /opt/openldap-2.4.40-cni/var/openldap-data

cachesize    20000
checkpoint   512    5
idlcachesize 100000
```

FIGURE 5.5 – configuration 1 du fichier slapd.conf

Puis on configure les ACLs pour gérer qui a les droits de voir le schéma, et qui peut s'authentifier à l'annuaire.

```

access to dn.base="" by * read
access to dn.base="cn=subschema" by * read

access to * attrs=userPassword
    by self write
    by users auth
    by anonymous auth

access to *
    by users read

loglevel 256

```

FIGURE 5.6 – configuration 2 du fichier slapd.conf

- **Création du schéma ldap et definition des classes d’objets**

Sous le répertoire schéma nous créons un fichier nommé CNI.schema, dont on définit les deux classes d’objets govPerson et govStructure, et on définit les attributs de chaque classe d’objet.

Pour la classe d’objet govStructure l’attribut obligatoire est le « ou » qui est d’après le tableau de conception de structure le ou est le nom de la structure. Les attributs secondaires sont tous le reste des attributs comme : [govWebsite postalAddress, facsimileTelephoneNumber, govAcronym, govAlias, govActivitySector, governorate ...]

```

objectclass ( CNIIDOC:2
    NAME 'govStructure'
    DESC 'govStructure represents structures in the tunisian government'
    AUXILIARY
    MUST ( ou )
    MAY ( govWebsite $ postalAddress $ telephoneNumber $
        facsimileTelephoneNumber $ govAcronym $ govAlias $
        govActivitySector $ governorate $ co $ govMunicipality $
        govDelegation $ mail $ govSocialNetwork $ govContact $
        govStructure $ govStructureType )
)
# attribute govStructureType

```

FIGURE 5.7 – Définition de la classe d’objet govStructure

Pour la classe d’objet govPerson l’attribut obligatoire est le « govCNRPS » qui est d’après le tableau de conception de personne le numero de de CNRPS. Les attributs secondaires sont tout le reste des attributs comme : [govCNSS ,govCIN ,govDegree, govFunction govFunctionStartDate , govDegreeStartDate ,govPositionStartDate, govSubPositionStartDate ...]

```

objectclass ( CNIODOC:1
  NAME 'govPerson'
  DESC 'govPerson represent people in the tunisian government'
  AUXILIARY
  MUST ( govCNRPS )
  MAY ( govCNSS $ govCIN $ govPosition $ govSubPosition $
        govDegree $ govFunction $ govFunctionStartDate $ govDegreeStartDate $
        govPositionStartDate $ govSubPositionStartDate $
        govBirthdate $ govFatherFirstName $ govGrandFatherFirstName $
        govMotherFirstName $ govMotherLastName $ co $ personalTitle )
)

```

FIGURE 5.8 – Définition de la classe d’objet govPerson

- **Définition des attributs et leurs syntaxes**

Dans le même fichier nommé CNI.schema on définit tous les attributs que nous avons saisie dans les classes d’objets.

```

#####
# Attributes
#####

# User attributes

attributetype ( CNIODAT:1 NAME ( 'govCNRPS' )
  DESC 'identifiant de Caisse Nationale de Retraite et de Prévoyance Sociale (sur 8 chiffres)'
  EQUALITY caseIgnoreMatch
  SYNTAX 1.3.6.1.4.1.1466.115.121.1.15
  SINGLE-VALUE )

attributetype ( CNIODAT:2 NAME ( 'govCNSS' )
  DESC 'identifiant de Caisse Nationale de Securite Sociale (sur 8 chiffres)'
  EQUALITY caseIgnoreMatch
  SYNTAX 1.3.6.1.4.1.1466.115.121.1.15
  SINGLE-VALUE )

attributetype ( CNIODAT:3 NAME ( 'govCIN' )
  DESC 'identifiant de Carte d Identite Nationale (sur 8 chiffres)'
  EQUALITY caseIgnoreMatch
  SYNTAX 1.3.6.1.4.1.1466.115.121.1.15
  SINGLE-VALUE )

attributetype ( CNIODAT:4 NAME ( 'govPosition' )
  DESC 'position actuelle de la personne'
  EQUALITY distinguishedNameMatch
  SYNTAX 1.3.6.1.4.1.1466.115.121.1.12 )

attributetype ( CNIODAT:5 NAME ( 'govSubPosition' )
  DESC 'sous-position actuelle de la personne'
  EQUALITY distinguishedNameMatch
  SYNTAX 1.3.6.1.4.1.1466.115.121.1.12 )

attributetype ( CNIODAT:6 NAME ( 'govDegree' )
  DESC 'grade de la personne'
  EQUALITY caseIgnoreMatch
  SUBSTR caseIgnoreSubstringsMatch
  SYNTAX 1.3.6.1.4.1.1466.115.121.1.15 )

attributetype ( CNIODAT:7 NAME ( 'govFunction' )
  DESC 'fonction de la personne'
  EQUALITY caseIgnoreMatch
  SUBSTR caseIgnoreSubstringsMatch
  SYNTAX 1.3.6.1.4.1.1466.115.121.1.15 )

```

FIGURE 5.9 – Définition des attributs de govPerson

Pour chaque attribut on définit son nom, sa description, le champ EQUALITY qui réfère à la méthode de recherche de cet attribut, sa syntaxe, et on dit si jamais il est multi-valeur ou un seule valeur.

De même manière on définit les attributs de la classe d'objet govStructure

```
# Structure attributes

attributetype ( CNIIDAT:50 NAME ( 'govWebsite' )
  DESC 'URL du site web de la structure'
  EQUALITY caseIgnoreMatch
  SUBSTR caseIgnoreSubstringsMatch
  SYNTAX 1.3.6.1.4.1.1466.115.121.1.15 )

attributetype ( CNIIDAT:51 NAME ( 'govAcronym' )
  DESC 'Sigle de la structure'
  EQUALITY caseIgnoreMatch
  SUBSTR caseIgnoreSubstringsMatch
  SYNTAX 1.3.6.1.4.1.1466.115.121.1.15 )

attributetype ( CNIIDAT:52 NAME ( 'govAlias' )
  DESC 'Alias de la structure'
  EQUALITY caseIgnoreMatch
  SUBSTR caseIgnoreSubstringsMatch
  SYNTAX 1.3.6.1.4.1.1466.115.121.1.15 )

attributetype ( CNIIDAT:53 NAME ( 'govActivitySector' )
  DESC 'secteur d activite de la structure (prise parmi une liste)'
  EQUALITY caseIgnoreMatch
  SUBSTR caseIgnoreSubstringsMatch
  SYNTAX 1.3.6.1.4.1.1466.115.121.1.15 )

attributetype ( CNIIDAT:54 NAME ( 'governorate' )
  DESC 'gouvernorat de la structure (prise parmi une liste)'
  EQUALITY caseIgnoreMatch
  SUBSTR caseIgnoreSubstringsMatch
  SYNTAX 1.3.6.1.4.1.1466.115.121.1.15 )

attributetype ( CNIIDAT:55 NAME ( 'govMunicipality' )
  DESC 'municipalite de la structure'
  EQUALITY caseIgnoreMatch
  SUBSTR caseIgnoreSubstringsMatch
  SYNTAX 1.3.6.1.4.1.1466.115.121.1.15 )

attributetype ( CNIIDAT:56 NAME ( 'govDelegation' )
  DESC 'delegation de la structure'
  EQUALITY caseIgnoreMatch
  SUBSTR caseIgnoreSubstringsMatch
  SYNTAX 1.3.6.1.4.1.1466.115.121.1.15 )

attributetype ( CNIIDAT:57 NAME ( 'govSocialNetwork' )
  DESC 'url du reseau social (twitter, facebook,...) de la structure'
  EQUALITY caseIgnoreMatch
  SUBSTR caseIgnoreSubstringsMatch
  SYNTAX 1.3.6.1.4.1.1466.115.121.1.15 )
```

FIGURE 5.10 – Definition des attributs de govStructure

Après configuration du serveur OpenLDAP , nous pouvons s'authentifier à ApacheDirectory Studio afin de commencer à remplir notre DIT.

La figure ci-dessous pressente l'interface de ApacheDirectory Studio à travers laquelle se connecte le rootdn qu'on a définie dans slapd.conf et remplit tous le informations nécessaires des structures, applications, personnes et infrastructure.

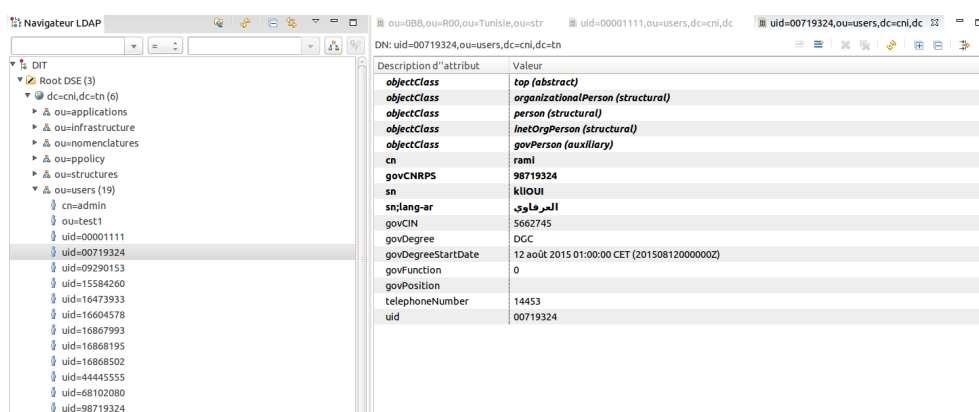


FIGURE 5.11 – Interface d'Apache Directory Studio

5.4 Navigation à travers LinID

Dans cette section nous allons montrer comment un utilisateur peut naviguer dans l'annuaire à travers LinID.

La figure ci-dessous pressente l'interface d'accueil de Linid après authentification via les cordonnées enregistrées dans l'annuaire déployé. Cette interface contient plusieurs rubriques, [recherche, personne, groupes, fonctionnalités, applications et structures].

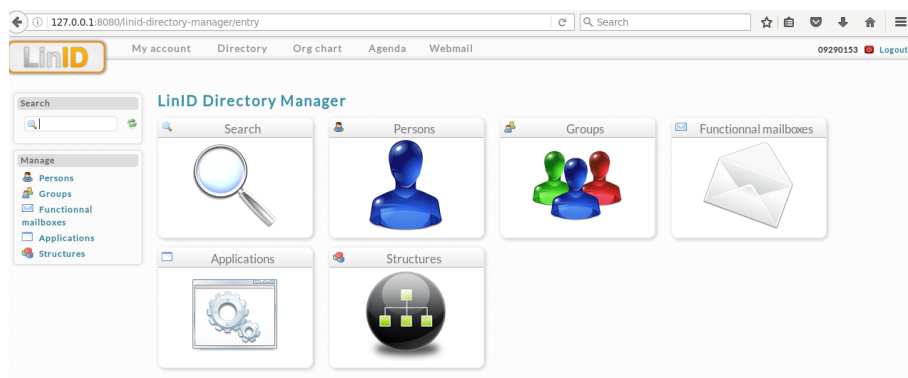


FIGURE 5.12 – Interface d'accueil de LINID

En accédant à la recherche, nous trouvons deux types de recherches :

- **Recherche par personne** : L'administrateur de l'établissement fixe les attributs de recherche d'une personne.

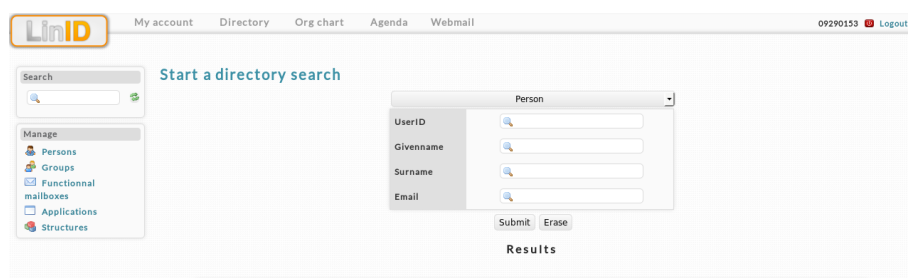


FIGURE 5.13 – Interface de Recherche d'une Personne

- **Recherche par structure** : L'administrateur de l'établissement fixe les attributs de recherche d'une structure.

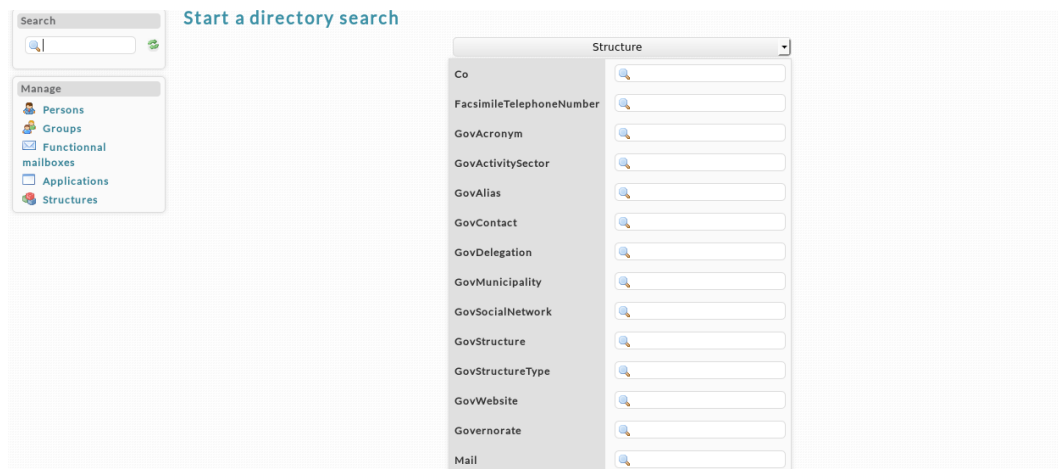


FIGURE 5.14 – Interface de Recherche d'une Structure

5.5 Conclusion

Dans ce chapitre Nous avons présenté l'environnement matériel et logiciel de notre projet , ainsi les taches réalisées dans la mise en place de l'annuaire. Dans le chapitre suivant nous allons poursuivre à présenter la réalisation du projet ainsi l'intégration de l'annuaire avec la plateforme de messagerie du Gouvernement Tunisien.

Conclusion Générale

Dans le cadre de la mise en œuvre des orientations nationales en matière de renforcement de l'utilisation des systèmes d'information nationales, le gouvernement Tunisien a mis comme objectif, l'instauration d'un système d'identification unique du citoyen qui se base principalement sur la notion d'annuaire et la mise en place d'une plateforme de messagerie et de partage de donnée qui est intégrée avec l'annuaire de l'état Tunisien.

Notre projet a consisté à concevoir le schéma d'annuaire, la conception de l'architecture globale dans une première étape, dans une deuxième étape l'installation des services, la configurations des différents serveurs, la préparation et l'importation des données existantes dans l'annuaire, et finalement la migration des applications sur l'annuaire LDAP unifié.

Ce stage nous a, en effet, permis d'avoir une autre image sur notre domaine d'étude et il nous a permis de mettre en pratique nos connaissances acquises tout au long de notre cursus d'études à Esprit.

Par le biais de ce stage, nous avons pu entrer en contact avec l'équipe de développement, intégration et administrateurs réseau et système de LINAGORA, commerciaux et managers chevronnés et dynamiques. Ceci nous a été très bénéfique, surtout, en ce qui concerne la façon d'aborder les problèmes et de concevoir les solutions, dans un esprit d'équipe et d'entraide, en prenant certaines responsabilités et en mettant en pratique nos connaissances théoriques.

En conclusion, ce projet nous a offert l'opportunité d'avoir un avant-gout sur la vie professionnelle et de nous familiariser avec la pratique et ses différentes contraintes.

Bien que la solution a été jugée satisfaisante, elle offre plusieurs perspectives d'amélioration. En effet ce projet est une première étape pour contribuer à un projet plus important relative à l'instauration d'une carte multi-services et multi-usage garantissant une identification et une authentification unique, forte et fiable du citoyen et permettant la centralisation de l'authentification en toute simplicité et sécurité aux différents services publics offerts.

Liste d'acronymes

- LPS : LINAGORA Pro Services
- LRS : LINAGORA Run Services
- LTS : LINAGORA Training Services
- CNI : Centre National de l'informatique
- Ministère des TIC : Ministère des Technologies de l'informatique et de la communication
- LDAP : Lightweight Directory Access Protocol
- DN : Distinguished Name
- RDN :Relative Distinguished Name
- DIT : Directory Information Tree
- TCP : Transmission Control Protocol
- ACL :Access Control List
- HTTP : Hypertext Transfer Protocol
- HTTPS : Hypertext Transfer Protocol Secure
- IP : Internet Protocol
- SSL : Secure Socket Layer

Bibliographie

- [1] Construire un annuaire d'entreprise avec LDAP, *Marcel Rizcallah*
- [2] Mastering OpenLDAP, Configuring, Securing, and integrating Directory Services, *[http ://obm.org/documentation](http://obm.org/documentation)*
- [3] Authentification forte auprès d'un serveur LDAP par la méthode SASL Kerberos, *Maryline MAKNAVICIUS-LAURENT*
- [4] OpenLDAP-initiation, *David Coutadeur*
- [5] OpenLDAP-avancée, *David Coutadeur*
- [6] Lemonldap NG-initiation, *Clement OUDET*

Netographie

[N1], <http://linagora.com>

[N2] <http://obm.org/documentation>

[N3], <http://linid.org/documentation>

[N4], <http://open-paas.org>

[N5], <http://thd.tn>

[N6], <http://web.mit.edu>

Annexe

Introduction

Dans ce dernier chapitre, nous allons présenter le déploiement d'une plateforme de messagerie et de partage de données et l'intégration de cette plateforme avec l'annuaire déployé.

Architecture matérielle

La plateforme de messagerie et de partage de documents sera déployée sur l'architecture matérielle suivante :

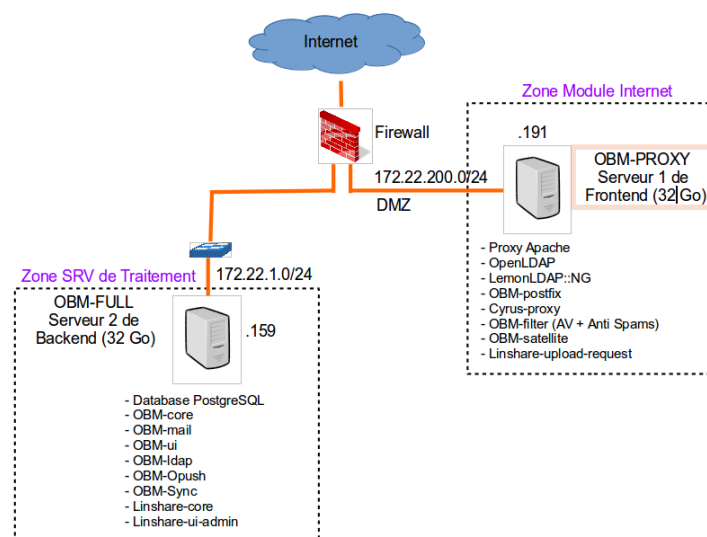


FIGURE 5.15 – Architecture matérielle

Composants de la solution

Nous allons détailler les différents composants de l'architecture :

- **Serveur 1(OBM-PROXY)** : C'est le même serveur physique dont nous avons installé l'annuaire. C'est un serveur Front End, il sera exposé à l'internet.
- **Serveur 1(OBM-FULL)** : Un serveur physique de 32 Go de mémoire vive fourni par le client, c'est le serveur de backend.
- **Proxy** : C'est le proxy « Front End », pour les services (SMTP, IMAP, POP3, HTTP); l'accès à cette machine se fait par Internet sur des protocoles sécurisés et authentifiés. De plus il héberge le service d'authentification unique SSO. Tous les autres services ne sont accessibles que par l'intermédiaire de ce serveur..
- **LemonLDAP : :NG** : Service qui assure le SSO (Single Sign On), la gestion des accès, la fédération d'identité et le partage de sessions sécurisées entre plusieurs applications.
- **OBM-mail** : Service de messagerie électronique « Back End Email » qui assure l'accès à la messagerie (IMAP, LMTP, SIEVE).
- **OBM-filtre** : Composant assurant le filtrage des e-mails malveillants par la biais de Amavisd couplé à SpamAssassin. Clamav est aussi couplé à Amavisd pour la protection anti-antivirus.
- **DATABASE** : Service qui assure l'accès en lecture et en ecriture aux bases de données.
- **OBM-core** : Groupe de packages qui compose le backend de OBM.
- **OBM-UI** : Service qui assure le rendu de l'interface WEB, il permet l'accès à la boîte mail, agenda, contacts, taches...
- **OBM-Ldap** : C'est un annuaire technique qui permet la gestion des bases d'adresses mails, des utilisateurs et des groupes ainsi que des hôtes OBM. Cet annuaire est entièrement géré par l'application et ne devrait pas être modifié sans passer par les API d'OBM.
- **OBM-Opush** : Service ActiveSync qui permet la synchronisation des comptes mails (emails, agenda et contacts) avec le mobile (iPhone, iPad, Android, Windows Phone...).

- **OBM-Sync** : Service de synchronisation des comptes mails (emails, agenda et contacts) avec les clients lourds (Thunderbird, Outlook...).
- **Linshare** : Service de partage de fichiers volumineux, avec une contrainte forte en terme de sécurité, entre les collaborateurs d'un même domaine mais également avec des correspondants externes.
- **Linshare-ui-admin** : Composant assurant le fonctionnement de l'interface d'administration de Linshare.

Matrice des flux

L'infrastructure fournie doit assurer la transmission des flux de données spécifiés dans la matrice des flux ci-jointe.

		MATRICE DE FLUX – SERVEUR DESTINATION		
		OBM-PROXY	OBM-FULL	INTERNET
MATRICE DE FLUX – SERVEUR SOURCE	OBM-PROXY		TCP / 22 TCP / 24 TCP / 80 TCP / 143 TCP / 389 TCP / 443 TCP / 636 TCP / 993 TCP / 4190 TCP / 8080 TCP / 8082 TCP / 8083 TCP / 8084 TCP / 8086	TCP / 25 TCP / 53 UDP / 53 TCP / 80 TCP / 110 UDP / 123 TCP / 143 TCP / 443 TCP / 465 TCP / 587 TCP / 873 TCP / 993 TCP / 995
	OBM-FULL	TCP / 22 TCP / 25 TCP / 143 TCP / 587 TCP / 30000 TCP / 3905		TCP / 53 UDP / 53 UDP / 123
	INTERNET	TCP / 25 TCP / 80 TCP / 110 TCP / 143 TCP / 443 TCP / 465 TCP / 587 TCP / 993 TCP / 995		

FIGURE 5.16 – Matrice des flux

Partitionnement des Serveurs

Serveur 1

Ci-dessous le dimensionnement de la machine 1 :

Partitions	Taille
/	20 Go
/boot	500 Mo
/var/log	20 Go
/tmp	20 Go
/var/lib/imap	5 Go
/usr/local/openldap	5 Go
/var/spool/postfix	10 Go
/var/lib/lemonldap-ng/conf	10 Go

FIGURE 5.17 – Partitionnement du serveur 1

Serveur 2

Ci-dessous le dimensionnement de la machine 2 :

Partitions	Taille
/	20 Go
/boot	500 Mo
/var/log	50 Go
/tmp	20 Go
/var/lib/inshare	1 To
/var/www	5 Go
/var/lib/imap	5 Go
/var/spool/imap	800 Go
/var/solr	10 Go
/var/lib/cassandra	20 Go
/var/lib/obm	30 Go
/var/lib/pgsql	100 Go

FIGURE 5.18 – Partitionnement du serveur 2

Solution finale

Dans cette section nous allons montrer avec des capture d'écrans la plateforme de messagerie après intégration avec l'annuaire déployé que nous avons cité dans les chapitres précédents.

Portail de la plateforme

Ci-dessous le le portail de la plateforme de messagerie du Gouvernement Tunisien, l'authetification se fait par les cordonnées suivantes :

Login : le mail ou le numero de CNRPS

par exemlpe : sami.hamila@tunisia.gov.tn ou 12345678.

Password : un mot de passe fournit par l'administrateur de l'établissement dont appartient l'utilisateur.

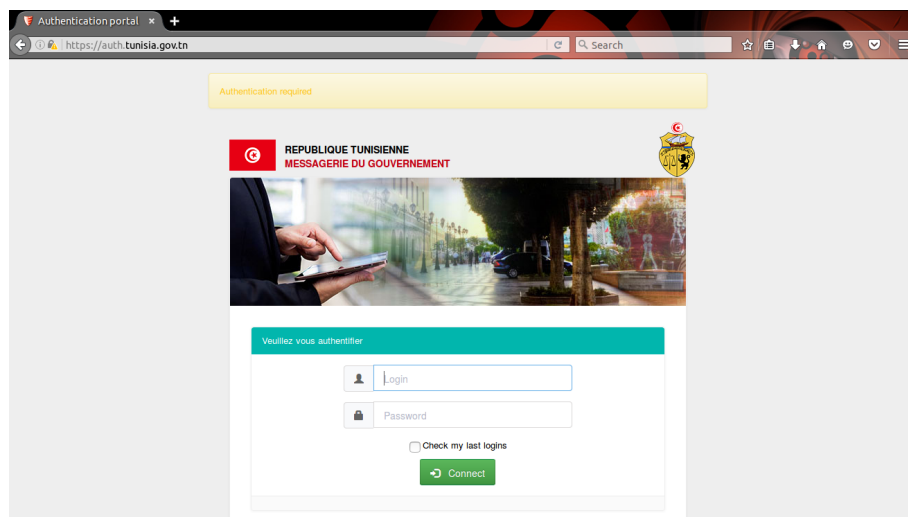


FIGURE 5.19 – Portail de la plateforme

Menu des applications

Après la phase de l'authentification, un menu apparait à l'utilisateur afin qu'il choisit l'application dont il veut y accéder.

A travers ce menu l'utilisateur peut accéder à la messagerie pour consulter sa boîte mail, envoyer des mails, créer des événements et les partager avec ses collègues , ainsi il peut ouvrir l'application Linshare dont il peut partager des fichiers d'une manière sécurisé.

Ci dessous la figure qui montre la liste des applications intégrées avec le WebSSO.

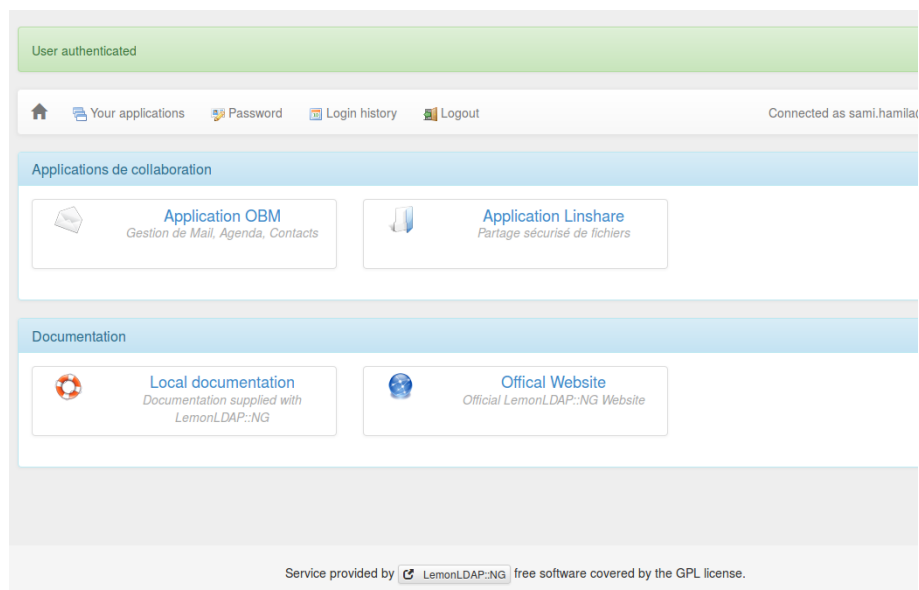


FIGURE 5.20 – Menu des applications

Application OBM

Ci-dessous la figure montre l’affichage du webmail :

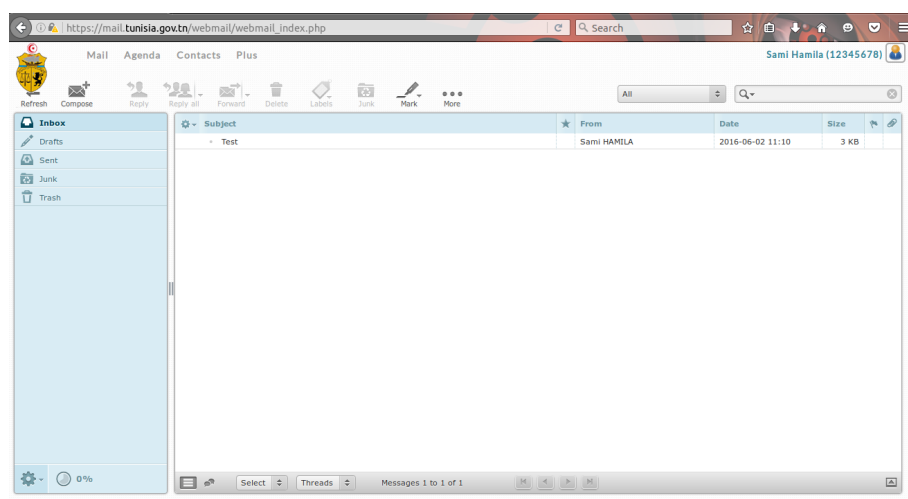


FIGURE 5.21 – Application OBM

Application Linshare

Ci-dessous la figure montre l’affichage de l’application Linshare : Chaque utilisateur a une la possibilité de partager et de recevoir des fichiers avec 100 Mo d’espace de stockage. Cet espace est variable, c’est un choix effectué par l’administrateur de chaque établissement.

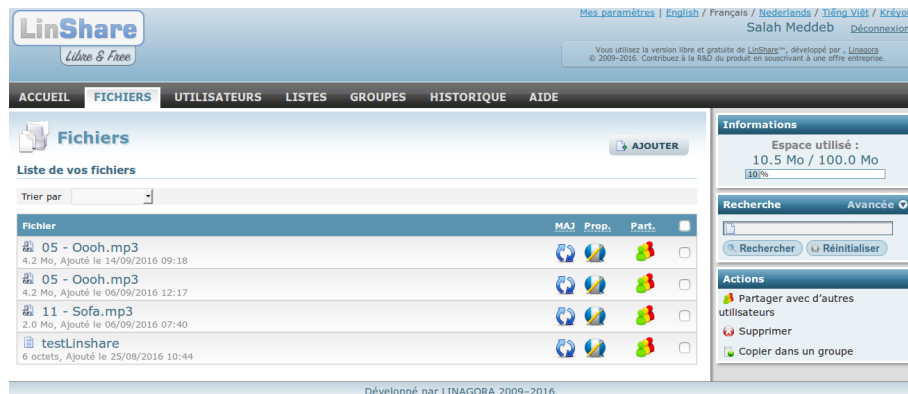


FIGURE 5.22 – Application Linshare

Conclusion

Dans cet annexe nous avons présenté l’architecture matérielle et nous avons énuméré les différents composants de la solution de l’intégration de l’annuaire et la plateforme de messagerie.