

MINISTERE DE L'ENSEIGNEMENT SUPERIEUR ET DE
LA RECHERCHE SCIENTIFIQUE
UNIVERSITE ABDELHAMID IBN BADIS - MOSTAGANEM

Faculté des Sciences Exactes et de l'Informatique
Département de Mathématiques et d'Informatique
Filière Informatique

MEMOIRE DE FIN D'ETUDES
Pour l'Obtention du Diplôme de Master en Informatique
Ingénierie des Systèmes d'Information

Mise en Œuvre d'une Messagerie Collaborative
Couplée à un ENT

Etudiante : BENMEKKI Amina

Directeur de mémoire : MOUSSA Mohamed

Année Universitaire 2017-2018

Résumé

Ce projet répond aux besoins de l'université de Mostaganem qui souhaite disposer d'un **Environnement Numérique de Travail** basé sur des produits **OpenSource**

Une messagerie collaborative OpenSource – ZIMBRA – est mise en œuvre avec un système d'authentification unifié CAS intégrée dans un ENT sous un environnement LINUX. L'administration et une description des principales fonctionnalités de Zimbra sont mises en exergue.

Mots clés : portail web, uPortal, SSO, CAS, messagerie collaborative, nextcloud

Remerciements

Mes sincères remerciements et ma gratitude à mon directeur de mémoire Monsieur Moussa Mohamed.

Giga remerciements à mes précieux frères Sofiane et Malik et à mon Daddy.

Table des matières

INTRODUCTION.....	9
1 ETAT DE L'ART.....	10
1.1 Introduction	10
1.2 Travail collaboratif.....	10
1.3 Intérêts du travail collaboratif	10
1.4 Types des outils de travail collaboratif.....	10
1.5 Messageries collaboratives.....	11
1.6 Produits Open Source.....	11
1.7 Zimbra	12
1.7.1 Architecture générale.....	12
1.7.2 Fonctionnalités de Zimbra.....	13
1.7.3 Possibilités d'intégration au niveau de Zimbra	14
1.8 Les Zimlets	15
1.9 Choix de Zimbra pour la faculté.....	16
2 SYSTEME D'AUTHENTIFICATION.....	17
2.1 Introduction	17
2.2 Système SSO	17
2.3 Fonctionnement	18
2.4 Système SSO CAS	19
2.4.1 Serveur CAS.....	19
2.4.2 Clients CAS.....	20
2.4.3 Protocole CAS.....	20
2.5 Mécanisme d'authentification	21
3 PREPARATION DE L'ENVIRONNEMENT DE TRAVAIL	22
3.1 Proxmox	22
3.2 VPN.....	23
3.3 OpenVPN	23
3.4 Secure Shell Protocol	24
3.5 Connexion au VPN.....	24
3.5.1 Accès à la machine uPortal.....	25
3.5.2 Accès à la machine Zimbra	26
3.6 Installation et configuration des différents services	27
3.6.1 uPortal	27
3.6.2 Zimbra	29
3.6.3 Nextcloud	34

3.7	Le SSO en action	36
3.7.1	Accès à une seconde application reliée au SSO	39
3.7.2	Déconnexion du SSO	41
3.8	Administration de uPortal, Zimbra et nextcloud	41
3.8.1	uPortal	41
3.8.2	Administration de Zimbra	45
3.8.3	Nextcloud	50
	CONCLUSION ET PERSPECTIVES	56
	Références et bibliographies	57

Listes des figures

Figure 1 : Architecture Générale de Zimbra	12
Figure 2 : Clients de Zimbra	14
Figure 3 : Zimlets disponibles par défaut sur Zimbra	15
Figure 4 : Système SSO	17
Figure 5 : CAS Protocol	21
Figure 6: Interface web d'authentification PROXMOX.....	22
Figure 7 : Serveurs utilisés	23
Figure 8 : Connexion au VPN	25
Figure 9 : Accès à la machine uPortal	26
Figure 10 : Accès à la machine Zimbra.....	27
Figure 11 : Nom d'hôte.....	29
Figure 12 : Résultat du FQDN	29
Figure 13 : configuration DNS (entrée de type A).....	30
Figure 14 : Résultat de install.sh	31
Figure 15 : Installation des Zimlets.....	31
Figure 16 : Fin de l'installation de Zimbra	32
Figure 17 : Interface Web de NEXTCLOUD	35
Figure 18 : URL de redirection au serveur CAS	37
Figure 19 : Formulaire d'authentification CAS	37
Figure 20 : Identification du profil après authentification	38
Figure 21 : Diagramme de séquence du premier accès via le SSO CAS	39
Figure 22 : URL d'accès à Zimbra via le SSO	40
Figure 23 : diagramme de séquence d'accès à la seconde application du SSO.....	40
Figure 24 : Appel de L'URL de déconnexion du serveur CAS	41
Figure 25 : Déconnexion du serveur CAS	41
Figure 26 : Interface utilisateur uPortal.....	42
Figure 27 : Portlet Email de Zimbra.....	42
Figure 28 : Portlet courses de uPortal	43
Figure 29 : Interface administrateur uPortal.....	44
Figure 30 : Outils d'administration uPortal	44
Figure 31 : URL de la console d'administration Zimbra.....	46
Figure 32 : Interface web administrateur	46
Figure 33 : Informations générales du compte.....	47
Figure 34 : Aliases.....	47
Figure 35 : caractéristiques du compte créé	48
Figure 36 : liste des comptes Zimbra	48
Figure 37 : Interface utilisateur Zimbra	49
Figure 38 : Interface d'authentification de Zimbra.....	49
Figure 39 : Page d'accueil d'un compte Zimbra	50
Figure 40 : Accès à nextcloud via Zimbra	50
Figure 41 : Interface d'authentification nextcloud.....	51
Figure 42 : Espace de partage de fichiers sous nextcloud.....	51
Figure 43 : Informations personnelles sous nextcloud.....	52

Figure 44 : Gestion des utilisateurs sous nextcloud	53
Figure 45 : Interface de l'api annonce	54
Figure 46 : Restrictions de l'annonce.....	54
Figure 47 : Interface de l'Annonce.....	55
Figure 48 : Interface TALK de nextcloud	55

Liste des tableaux

Tableau 1 : Ressources nécessaires pour uPortal	27
Tableau 2 : Ressources nécessaires pour Zimbra.....	29
Tableau 3 Commande line interface.....	45

INTRODUCTION

L'espace numérique de travail est une plateforme d'échanges qui rassemble tous les membres de la communauté d'un établissement universitaire. C'est un portail de services en ligne, c'est-à-dire un site web sécurisé offrant un point d'accès unique, qui a pour objectif de fournir à chaque utilisateur - enseignant, étudiant, administratif, technicien - un point d'accès unifié à l'ensemble des outils, contenus et services numériques en rapport avec son activité; il s'agit de rassembler toutes les fonctions disponibles dans un portail personnalisé adapté aux besoins de chacun : bureau numérique (annuaire, espace de stockage, agenda), outils de communication (messagerie), services de vie scolaire (emploi du temps, notes, absences , information administrative...). Ces fonctions seront accessibles à partir d'une identification unique.

Dans le cadre de notre projet, il s'agit de mettre en place un environnement de travail incluant une messagerie collaborative et un système d'authentification unifiée (SSO) cette authentification améliore directement la qualité du service rendu aux utilisateurs. Pour cela nous avons proposé la solution uPortal pour la mise en place de notre ENT et Zimbra comme messagerie collaborative, qui est un produit collaboratif OpenSource qui prend en charge les services de messagerie, calendrier, tâches, carnet d'adresses, ainsi que la gestion de documents.

1 ETAT DE L'ART

1.1 Introduction

La solution de messagerie collaborative offre des fonctionnalités indispensables pour optimiser le travail collaboratif entre l'ensemble des acteurs de l'activité. Nous allons présenter les notions du travail collaboratif ainsi que le produit choisi pour la mise en œuvre de notre messagerie.

1.2 Travail collaboratif

Le travail est souvent naturellement collectif et collaboratif, c'est-à-dire qu'il fait interagir plusieurs acteurs pour la réalisation de tâches qui visent à atteindre un but commun. La notion de travail collaboratif désigne aujourd'hui un travail qui n'est plus fondé sur l'organisation hiérarchisée traditionnelle, et plus spécifiquement un nouveau mode de travail où collaborent de nombreuses personnes grâce aux technologies de l'information et de la communication.

1.3 Intérêts du travail collaboratif

Le travail collaboratif présente des intérêts qui permettent la bonne conduite du projet collectif, certaines valeurs doivent être définies pour permettre de mener à bien le projet collaboratif parmi lesquelles :

- **Travail d'équipe** : mis en valeur grâce aux différents outils qui sont à la portée de tous les acteurs du travail collaboratif ;
- **Créativité** : qui est facilitée grâce aux différents échanges entre les membres du groupe de travail ;
- **Savoirs** : qui sont partagés car le travail de chaque personne reste à disposition du groupe.

1.4 Types des outils de travail collaboratif

Les outils de travail collaboratif peuvent se distinguer par leurs fonctionnalités :

- **Outils de communication** : les logiciels de courrier électronique sont utilisés à des fins d'échange, soit par listes de correspondants que l'on se crée soi-même dans le logiciel de courriel, soit par l'utilisation de listes de diffusion publique ou privée; nous pouvons également utiliser des logiciels de « chat » pour faciliter l'échange et le travail du groupe et un rapide partage d'informations, l'utilisation d'application TALK intégrée dans le service nextcloud permettra un échange audio/vidéo simultané et à plusieurs.

- **Outils de partage et de coordination** : ce sont des outils qui permettent de partager des fichiers dans un espace commun et de coordonner des tâches communes comme les agendas, gestions d'activité, annonces et sondages par exemple.

1.5 Messageries collaboratives

Les grandes solutions du marché se résument en deux catégories de produits :

- **Les produits propriétaires** : payants tels que Microsoft Exchange et Lotus.
- **Les produits OpenSource** : gratuits tels que Egroupware, OBM et Zimbra.

Notre choix s'est porté uniquement sur un produit Open source en particulier **Zimbra**

1.6 Produits Open Source

Les logiciels open source de messagerie électronique sont depuis longtemps utilisés, notamment pour leurs performances et leur disponibilité, étant capables d'héberger un nombre très important de boîtes aux lettres sur des configurations matérielles accessibles. Néanmoins, dès qu'on s'approche des besoins de messagerie collaborative (mobilité, agenda ...), ils ont longtemps accusé un retard important, soit sur le plan fonctionnel, soit sur le plan ergonomique. Aujourd'hui, l'éventail de technologies et de solutions est plus large, et des clients de messagerie comme **Thunderbird**, de la fondation Mozilla, progressent à grande vitesse. Les alternatives au couple Exchange/Outlook sont donc de plus en plus intéressantes, et toujours aussi accessibles.

Outre les possibilités d'échange de courriels et de gestion des boîtes aux lettres, les solutions open source intègrent désormais les services d'**annuaire** d'entreprise, les meilleures protections par **antivirus** et antispam, et les fonctionnalités **d'agenda** et de calendrier partagé. Ils intègrent aussi un **Webmail** de grande qualité pour donner accès à la messagerie à vos utilisateurs nomades et à vos clients légers. Le mail serveur supporte la plupart des protocoles de messagerie, il permet une grande capacité de stockage des messages et supporte la gestion des quotas¹.

1.7 Zimbra

Zimbra Collaboration Suite ZCS est l'une des premières solutions de gestion de messagerie et de travail collaboratif complète au monde aux côtés de Microsoft Exchange et Lotus Notes², de plus elle offre une solution intégrant tous les composants essentiels d'une messagerie incluant les composants de sécurité et le client Web très évolué AJAX.

1.7.1 Architecture générale

Zimbra peut gérer plusieurs centaines de milliers de comptes de messagerie sur un serveur qui est conçu à partir de briques open source (Linux, Apache, Postfix, MySQL, OpenLDAP...), et bénéficie d'une architecture extrêmement stable et modulaire.

Les différentes briques sont intégrées pour une installation facile et rapide du serveur Zimbra qui utilise les protocoles ouverts standards dans l'industrie (SMTP, LMTP, SOAP, XML, IMAP, POP, iCal, CalDAV) et peut s'installer sur les principales distributions Linux du marché (Red Hat Enterprise, Fedora, Ubuntu, Debian, Mandriva, and SUSE Linux) ou sur Mac OS X, rPath ou VMware. Le serveur Zimbra est 3 à 5 fois plus rapide que les systèmes comparables.

Chaque serveur possède son propre stockage des e-mails et des comptes. Pour monter en charge, il suffit d'ajouter des serveurs supplémentaires.

L'architecture de Zimbra est illustrée dans la figure ci-dessous ³:

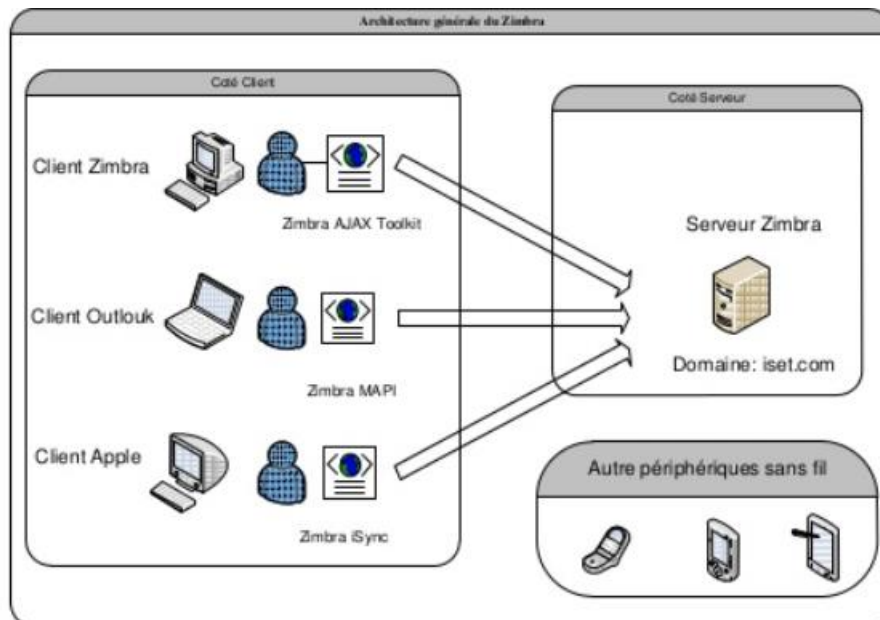


Figure 1 : Architecture Générale de Zimbra

1.7.2 Fonctionnalités de Zimbra

Zimbra est une solution complète qui comprend les fonctionnalités suivantes :

- Un client Web :

Zimbra dispose d'une particularité forte : il est développé sur un mode « Web service », toute l'interface AJAX est chargée à la première connexion, puis les interactions, les ajouts et les modifications d'informations sont envoyées au serveur par le protocole SOAP (simple Object Access protocole, son interface AJAX pour client web permet de disposer d'une interface autorisant le glisser/déposer, le clic-droit, les infobulles, l'utilisation de raccourcis clavier, le rendant très simple à utiliser, le serveur est accessible via tout navigateur web moderne et de nombreux clients lourds tel que Mozilla Thunderbird et Outlook Express uniquement pour ce qui est de l'annuaire (via LDAP «lightweight Directory Access Protocol») ou les emails (via POP3 «post office Protocol» ou IMAP «Internet Message Access Protocol»).

- Autres clients de messagerie :

Zimbra offre la compatibilité aux clients de messagerie, donne aux utilisateurs une meilleure liberté de choix, Mac et les environnements de bureau Linux sont pris en charge sur le même serveur Zimbra.

- Synchronisation MAPI (Messagerie Application Programming Interface) native avec Outlook (avec délégation et accès hors-ligne).
- Synchronisation native avec les applications Apple Desktop (connecteur Zimbra iSync)
- Clients support: Outlook, Thunderbird, Apple Mail, Sunbird, Novell Evolution.

Quelques exemples clients de messagerie sont illustrés dans la figure suivante ⁴:

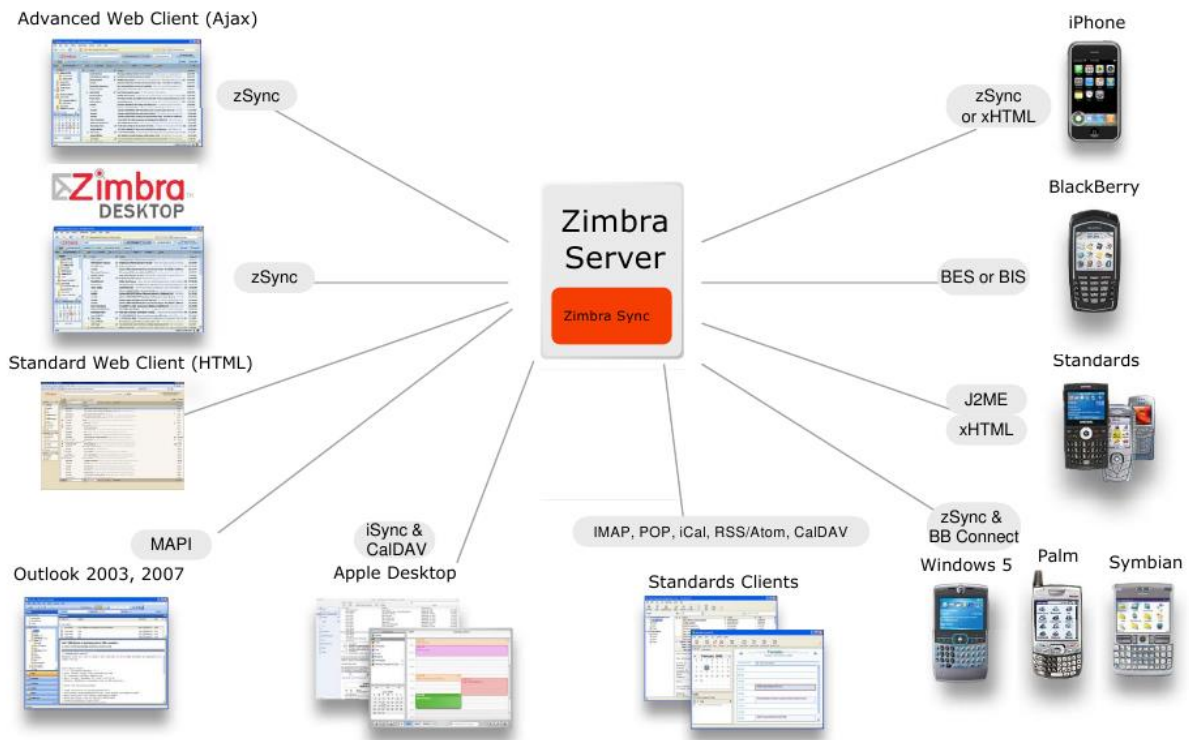


Figure 2 : Clients de Zimbra

- Accès mobiles :

L'accès mobile (smartphones et PDA «Personal digital Assistant») est intégré dans Zimbra Collaboration Suite, le client lourd Desktop permet d'effectuer une synchronisation de son compte de messagerie sur son poste de travail et d'y accéder en mode offline si besoin, Zimbra peut être consulté à partir d'un large éventail d'appareils, des téléphones du marché de masse pour Smartphones.

- Administration :

Zimbra offre aux administrateurs des fonctionnalités avancées comme la sauvegarde, la restauration et le déplacement de boîtes aux lettres « online », l'intégration avec des annuaires LDAP existants, la possibilité de fonctionner en cluster ainsi que l'intégration à des web services déjà existant ; de même, il intègre un antispam et un antivirus.

1.7.3 Possibilités d'intégration au niveau de Zimbra

Grâce à son infrastructure basée sur des logiciels libres, Zimbra permet une intégration avancée dans les systèmes d'information. Au-delà d'une «brique collaborative», Zimbra permet de disposer d'un environnement collaboratif, et ainsi construire un flux d'informations métier organisé et automatisé, permettant de rendre vraiment service aux différents collaborateurs.

Cette solution propose dans ce cadre de nombreux services avancés, tels que :

- Intégration dans votre annuaire d'établissement, afin de n'administrer qu'un seul annuaire,
- Intégration d'un environnement de SSO (Single Sign-On) permettant une authentification unique depuis un portail applicatif.
- Intégration de services de GED (Gestion Electronique de Documents)

1.8 Les Zimlets

Un zimlet est un add-on (composant logiciel) qui permet à Zimbra (ZCS) de disposer de nouvelles fonctionnalités ⁵ qui vont être intégrées dans l'interface utilisateur et cela de façon très rapide, bien évidemment, ZCS fournit en standard un certain nombre de Zimlets, mais il est également possible de développer ses propres Zimlets. (Api XML, Javascript, côté client), soit simplement avec l'installation d'un zimlet existant que nous pouvons retrouver dans une galerie sur internet prêts à être déployés.

Exemples de Zimlets disponibles :

- intégration avec des CRM comme SugarCRM, Salesforce,
- intégration avec Alfresco,
- ajout de Google Map ou Yahoo! directement dans Zimbra,
- ajout du moteur de traduction Google,
- intégration avec Facebook, Tweeter...

Les Zimlets qui sont déployés par défaut sur Zimbra sont illustrés dans la figure suivante :

Home - Configure - Zimlets ? Help ⚙️				
Name	Display Name	Descrip...	Version	Status
com_zextras_chat_open		OpenChat ...	10	Disabled
com_zextras_drive_open	Zimbra Drive	Cloud inte...	2.0.1	Disabled
com_zimbra_attachcontacts	Attach Contacts	Allows Atta...	1.1	Enabled
com_zimbra_attachmail	Email Attacher	Attach em...	1.2	Enabled
com_zimbra_date	Date	Highlights ...	2.7	Enabled
com_zimbra_email	Email	Highlights ...	11.12	Enabled
com_zimbra_mailarchive	Archive	One button...	0.6	Enabled
com_zimbra_phone	Phone	Highlights ...	2.7	Enabled
com_zimbra_srchhighlighter	Search Highlighter	After a mai...	0.9	Enabled
com_zimbra_url	URL Links	Highlight ...	2.5	Enabled
com_zimbra_webex	WebEx	Easily sch...	3.4	Enabled
com_zimbra_ymemoticons	Yahoo! Emoticons	Displays Y...	2.10	Enabled

Figure 3 : Zimlets disponibles par défaut sur Zimbra

1.9 Choix de Zimbra pour la faculté

Zimbra est une solution approuvée par de nombreuses Universités étrangères pour plusieurs raisons dont nous citerons les principales :

- **Administration et maintenance simplifiées** : Zimbra permet de gérer l'ensemble d'une communauté d'utilisateurs (étudiants, employés et professeurs) à partir d'une installation unique et tout cela à partir d'une interface Web.
- **Solution accessible via n'importe quel périphérique** : Zimbra se synchronise avec l'ensemble des smartphones disponibles, ainsi qu'avec les clients lourds traditionnels comme Microsoft Outlook via MAPI
- **Solution open source** : de par la nature de sa licence Zimbra peut être intégré à votre parc applicatif sans aucune contamination virale contrairement à des technologies propriétaires. Zimbra peut être installé sur un serveur Linux (Unix).
- **Sauvegardes et restauration simple et efficaces** : Zimbra permet de faire des sauvegardes en temps réel et de les gérer directement à partir de l'interface web d'administration.
- **Antivirus et anti spam intégrés** : ClamAV et Spam Assassin, des logiciels Open Source reconnus pour leurs efficacités, sont intégrés dans le paquet d'installation de Zimbra.
- **Communication sécurisée** : S/MIME permet l'encryption des courriels et l'utilisation de signature digitale.
- **Sécurité des données** : les données sont hébergés dans des data-centers réunissant des conditions de sécurité idéale. Des sauvegardes sont aussi réalisées afin de garantir la protection des données.

2 SYSTEME D'AUTHENTIFICATION

2.1 Introduction

L'objectif est de comprendre les prérequis logiciels et matériels et aussi de connaître les différentes phases d'installation, d'configuration et d'administration de notre serveur de messagerie Zimbra avec intégration de nextcloud et du portail web uPortal.

2.2 Système SSO

C'est un système d'authentification qui permet à l'utilisateur de pouvoir accéder à de nombreuses applications sans avoir à multiplier les authentifications. « Single Sign-On », qui veut bien dire qu'il n'y a qu'une seule ("single") connexion ("Sign-on").⁶

Ce système se compose de plusieurs éléments :

- **Le client** : un navigateur web.
- **Le serveur d'authentification** : l'élément central du système SSO, assure l'authentification de l'utilisateur, la persistance de sa connexion et la propagation de l'identité de l'utilisateur auprès des applications.
- **Le serveur d'application** : qui lui ne délivre les ressources qu'après s'être assuré que le navigateur (le client) qui l'accède se soit authentifié auprès du serveur d'authentification.

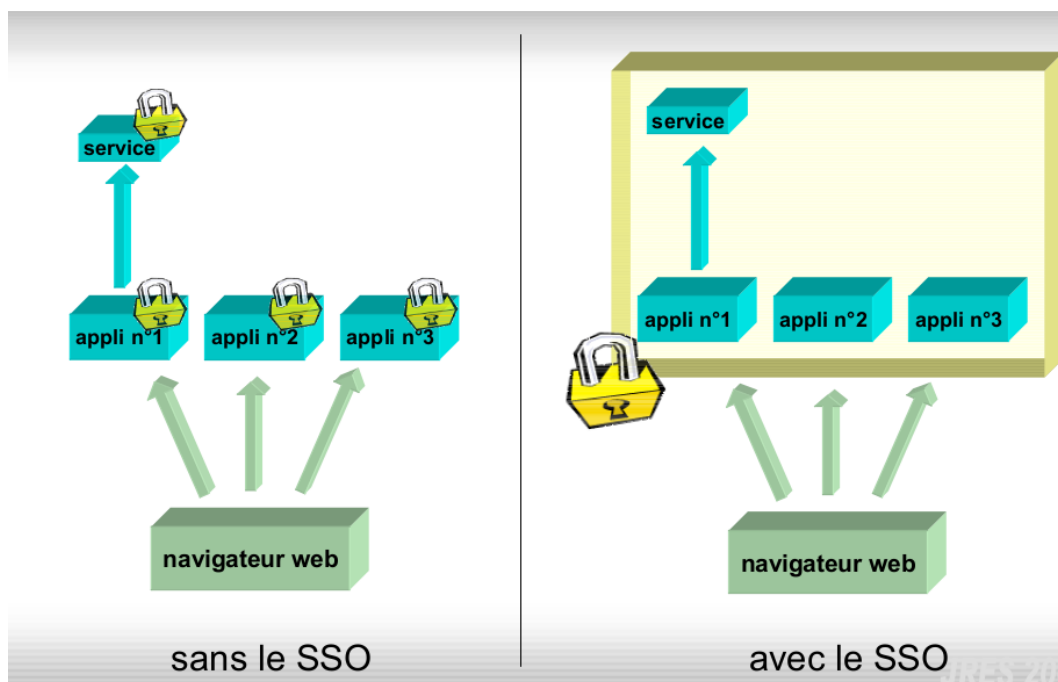


Figure 4 : Système SSO

2.3 Fonctionnement

L'utilisateur renseigne un mot de passe en début de session et peut ensuite accéder à de nombreuses applications informatiques sans être contraint de devoir s'authentifier sur chacune d'entre elles. Les étapes pour accéder à une application dans un système SSO sont les suivantes :

1. accès à l'application dont l'authentification est déléguée au service d'authentification SSO ;
2. redirection de l'utilisateur vers le serveur d'authentification ;
3. identification et authentification de l'utilisateur par le serveur d'authentification ;
4. redirection de l'utilisateur vers l'application ;
5. accès à l'application.

Un jeu de va-et-vient à lieu entre le serveur d'authentification et l'utilisateur puis entre le serveur d'authentification et le serveur d'application pour vérifier les droits de l'utilisateur sur l'application à laquelle il veut accéder :

- **Du côté de l'annuaire et de la gestion des droits**

L'utilisateur doit être inscrit dans l'annuaire d'entreprise pour être ensuite habilité à accéder aux diverses applications auxquelles il a droit. La gestion des droits se fait ensuite via un outil du SSO qui va permettre de gérer les droits des utilisateurs répertoriés dans l'annuaire.

- **Du côté de l'utilisateur**

L'utilisateur accède à la page d'authentification soit par accès volontaire via un portail d'accès aux applications soit par une redirection suite à une tentative d'accès à une application sans authentification préalable. Il s'identifie en saisissant son login et son mot de passe. Ensuite, l'accès au serveur application se fera depuis les liens du portail d'accès ou directement si l'utilisateur connaît le lien.

- **Du côté de l'application**

Le serveur d'application est protégé par un " agent d'authentification " :

- l'agent intercepte chaque tentative d'accès à l'application et vérifie que l'utilisateur est authentifié (par exemple, la présence d'un cookie sur le poste de travail),
- il s'assure ensuite auprès du serveur d'authentification que l'utilisateur est autorisé à accéder à la partie demandée de l'application.

2.4 Système SSO CAS

Le SSO CAS (acronyme de Central Authentication Service) est une solution d'authentification centralisée open source originellement développée par l'université de Yale et reprise depuis par Jasig, qui est très répandue dans les réseaux intranet d'universités, mais également utilisée dans certaines entreprises⁷.

L'architecture d'un système basé sur CAS est très simple : comme le CAS est écrit en Java, nous avons simplement besoin d'un serveur d'applications (Jetty, Tomcat, etc.) déployer CAS.

Le serveur CAS et les clients comprennent les deux composants physiques de l'architecture du système CAS qui communiquent au moyen de divers protocoles.

2.4.1 Serveur CAS

Le serveur CAS est responsable de l'authentification des utilisateurs et de l'octroi d'accès aux applications. Celui-ci est une servlet Java basée sur Spring Framework, dont la responsabilité principale est d'authentifier les utilisateurs et d'accorder l'accès aux services CAS, communément appelés clients CAS, en émettant et en validant des tickets. Une session SSO est créée lorsque le serveur émet un ticket d'octroi de ticket (TGT) à l'utilisateur lors de la connexion réussie. Un ticket de service (ST) est délivré à un service à la demande de l'utilisateur

via des redirections de navigateur en utilisant le TGT en tant que jeton. Le ST est ensuite validé sur le serveur CAS via une communication de retour. Ces interactions sont décrites en détail dans le document du Protocole CAS.

2.4.2 Clients CAS

Le terme "client CAS" a deux significations distinctes dans son usage commun. Un client CAS est une application compatible CAS qui peut communiquer avec le serveur via un protocole pris en charge. Un client CAS est également un progiciel qui peut être intégré à diverses plates-formes logicielles et applications afin de communiquer avec le serveur CAS via un certain protocole d'authentification (par exemple CAS, SAML, Auth). Des clients CAS prenant en charge un certain nombre de plates-formes et de produits logiciels ont été développés.

Platforms :

- Apache httpd Server (mod_auth_cas module)
- Java (Java CAS Client)
- .NET (.NET CAS Client)
- PHP (phpCAS)
- Perl (PerlCAS)
- Python (pycas)
- Ruby (rubycas-client)

Applications :

- Outlook Web Application (ClearPass + .NET CAS Client)
- Atlassian Confluence
- Atlassian JIRA
- Drupal
- Liferay
- UPortal

2.4.3 Protocole CAS

Le protocole CAS est un protocole simple et puissant basé sur des tickets développés exclusivement pour CAS. Les clients sont intégrés dans des applications CASified (appelées "services CAS") alors que le serveur CAS est un composant autonome.

Protocole CAS : la cinématique

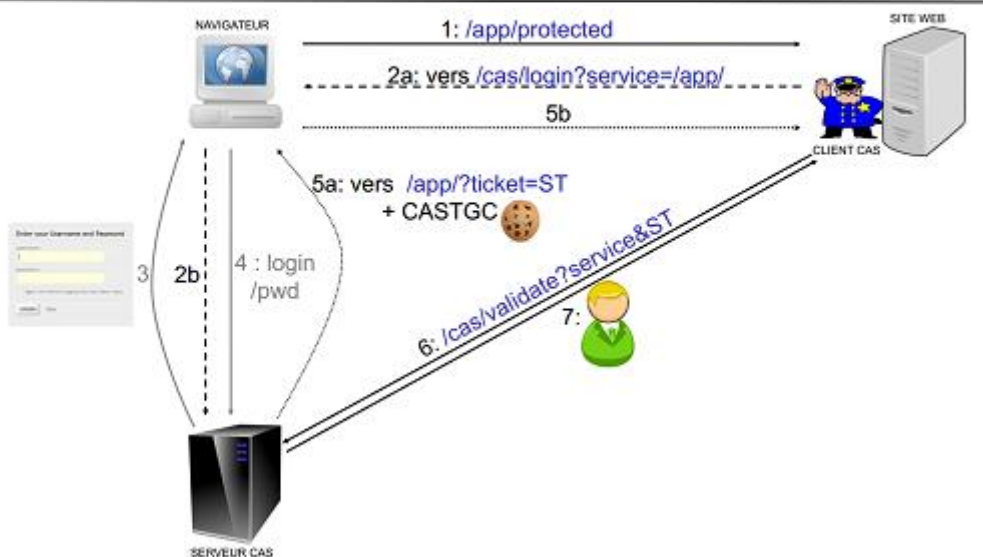


Figure 5 : CAS Protocol

Concepts clés :

- Le TGT (Ticket Granting Ticket), stocké dans le cookie CASTGC, représente une session SSO pour un utilisateur.
- Le ST (Service Ticket), transmis en tant que paramètre GET dans les URL, représente l'accès accordé par le serveur CAS à l'application CASified pour un utilisateur spécifique.

2.5 Mécanisme d'authentification

Nous allons utiliser le protocole CAS comme protocole d'authentification entre les applications suivantes :

Zimbra : en utilisant le webservice preauth.⁸

uPortal : un client CAS Jasig est présent sur le produit.

Nextcloud : le client CAS est intégré nativement depuis la version 11+.

3 PREPARATION DE L'ENVIRONNEMENT DE TRAVAIL

Afin de mettre en place les différents services, nous avons mis en place une petite infrastructure composée de trois machines virtuelles. Les sections suivantes décrivent les services et protocoles utilisés.

3.1 Proxmox

Proxmox est une solution complète de gestion de virtualisation de serveur open source. Il offre la possibilité de gérer la technologie de serveur virtuel (VPS) avec les technologies Linux OpenVZ et KVM. Proxmox propose une interface web accessible après l'installation sur votre serveur, ce qui facilite la gestion, ne nécessitant généralement que quelques clics. C'est une solution open source, elle peut être personnalisée selon les besoins⁹.

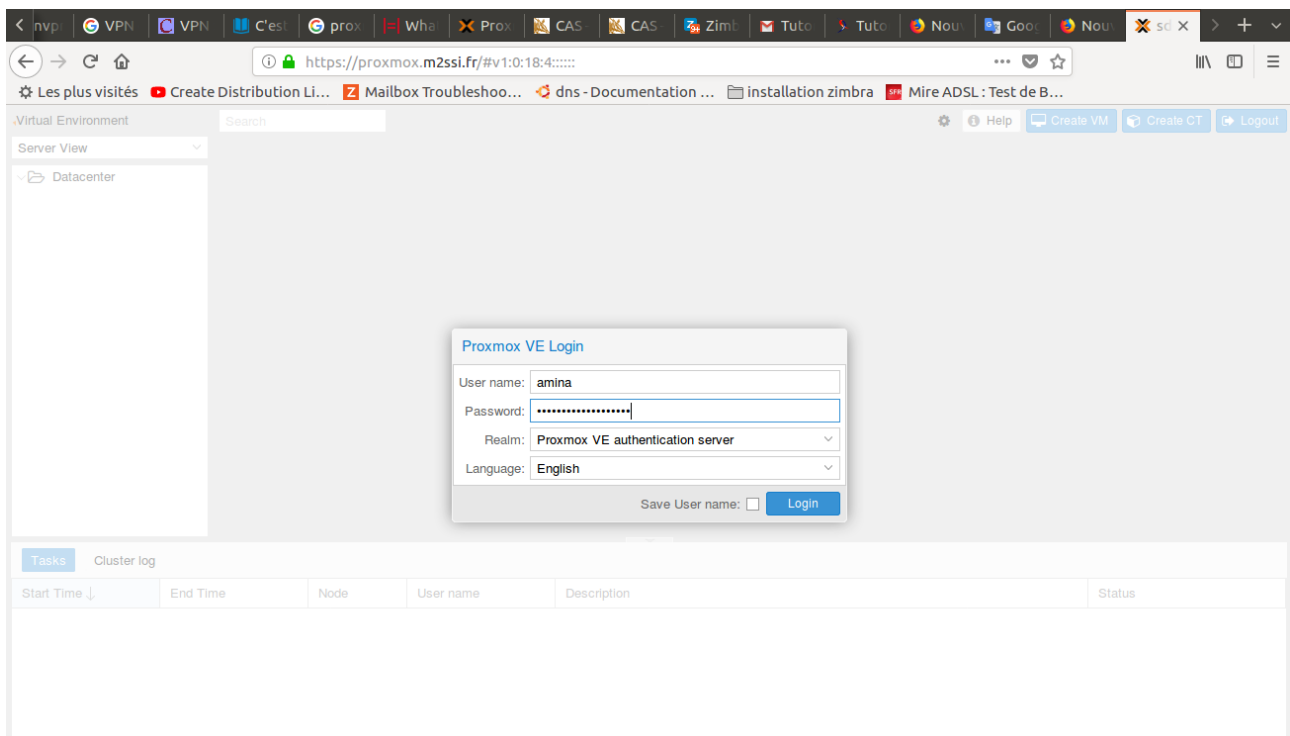


Figure 6: Interface web d'authentification PROXMOX

Illustrations des informations sur les trois machines utilisées

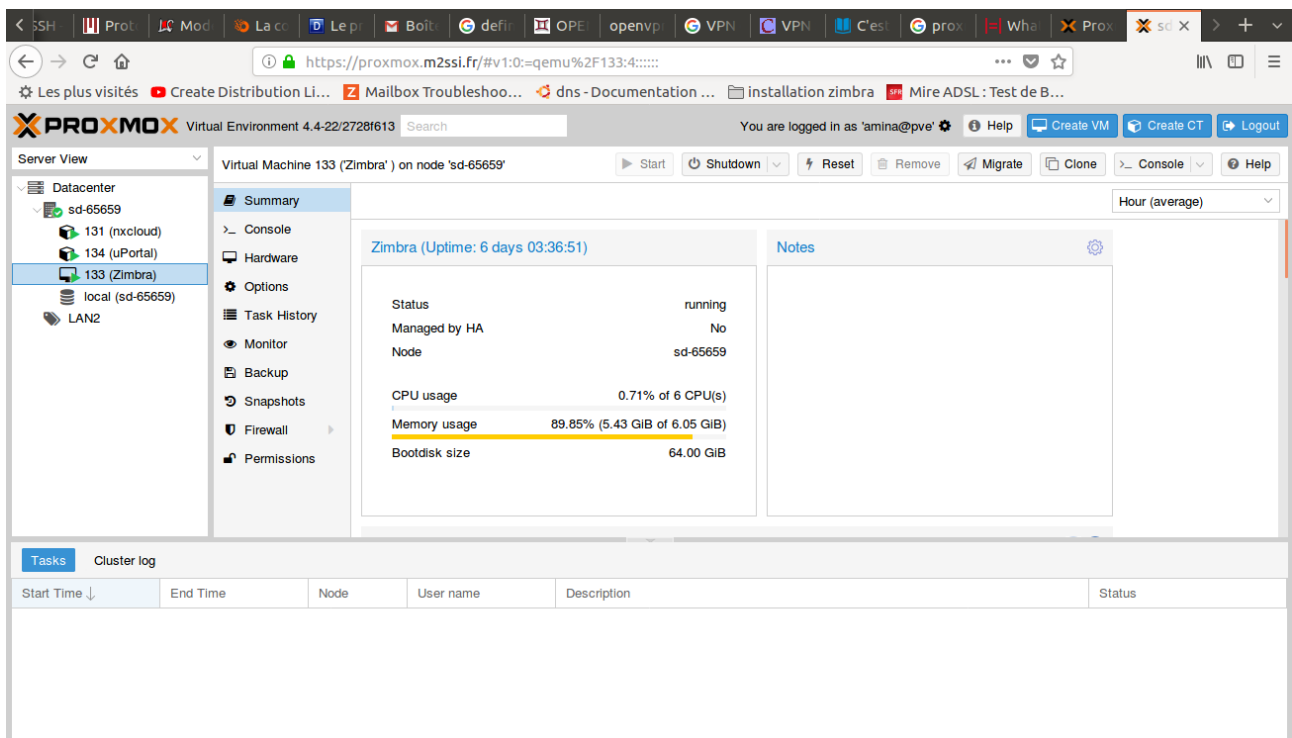


Figure 7 : Serveurs utilisés

3.2 VPN

Le VPN ou Virtual Privat Network est une connexion inter réseau permettant de masquer une partie de son réseau privé au reste du réseau public. Une entreprise ne déploie pas tout son réseau informatique sur le réseau internet public, une partie est installée sur le réseau interne, sur des adresses internet internes. Ce réseau n'est pas accessible depuis l'internet public, mais depuis une machine ayant accès au réseau interne. Ce réseau est donc privé. Étant simplement un jeu d'adresses réseau, il est aussi virtuel. Cette technologie a été utilisée afin d'accéder au réseau privé des machines virtuelles¹⁰

3.3 OpenVPN

OpenVPN est un logiciel libre permettant de créer un réseau privé virtuel (VPN) et un outil de création de VPN conviviale, robuste et facilement configurable. Il peut être utilisé pour relier de manière sécurisée deux ou plus réseaux privés, en utilisant un tunnel chiffré à travers Internet. Il est le seul produit VPN open source à supporter entièrement l'ICP¹¹(Infrastructure à Clef Publique). Le logiciel contient un exécutable pour les connexions du client et du serveur, un fichier de configuration optionnel et une ou plusieurs clés suivant la méthode d'authentification choisie.

3.4 Secure Shell Protocol

Le protocole ssh (**Secure Shell**) est utilisé pour établir un accès sécurisé permettant d'effectuer des opérations sur des machines distantes et des transferts de fichiers à travers un réseau public tout en garantissant l'authentification, la confidentialité et l'intégrité des données. L'authentification¹²

Une fois que la connexion sécurisée est mise en place entre le client et le serveur, le client doit s'identifier sur le serveur afin d'obtenir un droit d'accès. Il existe plusieurs méthodes :

- La méthode la plus connue est le traditionnel mot de passe. Le client envoie un nom d'utilisateur et un mot de passe au serveur au travers de la communication sécurisée et le serveur vérifie si l'utilisateur concerné a accès à la machine et si le mot de passe fourni est valide.
- Une méthode moins connue, mais plus souple est l'utilisation de clés publiques. Si l'authentification par clé est choisie par le client, le serveur va créer un *challenge* et donner un accès au client si ce dernier parvient à déchiffrer le challenge avec sa clé privée.

Dans notre cas nous avons utilisé la méthode du traditionnel mot de passe pour accéder aux machines distantes.

3.5 Connexion au VPN

Entrer en mode root : super utilisateur, c'est-à-dire en tant qu'administrateur système on aura tous les droits sur l'appareil et on pourra modifier tous les éléments de l'OS y compris les fichiers sensibles, pour se connecter au VPN, il faut lancer un terminal en root et se positionner dans le dossier « /home/amina/pfSense-TCP-1195 » et d'exécuter la commande suivante :

```
openvpn --config pfSense-TCP-1195.ovpn
```



```
root@mail: /home/amina/pfSense-TCP-1195
amina@mail:~$ sudo -i
[sudo] Mot de passe de amina :
root@mail:~# cd /home/amina/pfSense-TCP-1195/
root@mail:/home/amina/pfSense-TCP-1195# openvpn --config pfSense-TCP-1195.ovpn
Sun May 13 19:40:52 2018 OpenVPN 2.3.10 x86_64-pc-linux-gnu [SSL (OpenSSL)] [LZO] [EPOL
L] [PKCS11] [MH] [IPv6] built on Jun 22 2017
Sun May 13 19:40:52 2018 library versions: OpenSSL 1.0.2g  1 Mar 2016, LZO 2.08
Enter Auth Username: *****
Enter Auth Password: *****
Sun May 13 19:41:18 2018 WARNING: file 'pfSense-TCP-1195-tls.key' is group or others ac
cessible
Sun May 13 19:41:18 2018 Control Channel Authentication: using 'pfSense-TCP-1195-tls.ke
y' as a OpenVPN static key file
Sun May 13 19:41:18 2018 Attempting to establish TCP connection with [AF_INET]62.210.86
.32:1195 [nonblock]
Sun May 13 19:41:19 2018 TCP connection established with [AF_INET]62.210.86.32:1195
Sun May 13 19:41:19 2018 TCPv4_CLIENT link local (bound): [undef]
Sun May 13 19:41:19 2018 TCPv4_CLIENT link remote: [AF_INET]62.210.86.32:1195
Sun May 13 19:41:19 2018 WARNING: this configuration may cache passwords in memory -- u
se the auth-nocache option to prevent this
Sun May 13 19:41:20 2018 [proxmox.m2ssi.fr] Peer Connection Initiated with [AF_INET]62.
210.86.32:1195
Sun May 13 19:41:22 2018 TUN/TAP device tun1 opened
Sun May 13 19:41:22 2018 do_ifconfig, tt->ipv6=0, tt->did_ifconfig_ipv6_setup=0
Sun May 13 19:41:22 2018 /sbin/ip link set dev tun1 up mtu 1500
Sun May 13 19:41:22 2018 /sbin/ip addr add dev tun1 10.9.9.4/24 broadcast 10.9.9.255
RTNETLINK answers: File exists
Sun May 13 19:41:22 2018 ERROR: Linux route add command failed: external program exited
with error status: 2
Sun May 13 19:41:22 2018 Initialization Sequence Completed
```

Figure 8 : Connexion au VPN

Une fois connecté au VPN, il est possible de communiquer directement avec les machines virtuelles et ainsi d’y accéder.

3.5.1 Accès à la machine uPortal

Cette machine contient l’instance de l’ENT uPortal. L’accès à celle-ci peut se faire en SSH en utilisant les informations suivantes :

IP : 192.168.5.134

Utilisateur SSH : root

Commande SSH : ssh userssh@192.168.5.134

```
amina@mail: ~
amina@mail:~$ ssh root@192.168.5.134
root@192.168.5.134's password:
Linux uPortal 4.4.98-6-pve #1 SMP PVE 4.4.98-107 (Fri, 16 Feb 2018 10:11:56 +0100) x86_64

The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
Last login: Sun May 13 14:50:02 2018 from 10.9.9.3
root@uPortal:~#
```

Figure 9 : Accès à la machine uPortal

3.5.2 Accès à la machine Zimbra

Cette machine contient l'instance de Zimbra. L'accès à celle-ci peut se faire en SSH en utilisant les informations suivantes :

IP :192.168.5.133

Utilisateur SSh : amina

Commande SSH : ssh amina@192.168.5.133

```

amina@mail:~$ ssh amina@192.168.5.133
amina@192.168.5.133's password:
Welcome to Ubuntu 16.04.4 LTS (GNU/Linux 4.13.0-36-generic x86_64)

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

99 paquets peuvent être mis à jour.
0 mise à jour de sécurité.

*** Le système doit être redémarré ***
Last login: Sun May 13 16:50:26 2018 from 10.9.9.3
amina@zimbra:~$

```

Figure 10 : Accès à la machine Zimbra

3.6 Installation et configuration des différents services

Les différentes machines en place et accessibles, il est temps de passer à l'installation des différents services.

3.6.1 uPortal

uPortal-start est le mécanisme par lequel les individus et les institutions adoptent Apereo uPortal, le principal portail d'entreprise open source construit par et pour les établissements d'enseignement supérieur ¹³, afin de faciliter la mise en place du portail nous allons utiliser uPortal-start pour déployer uPortal, en utilisant uPortal-start nous allons disposer des tâches gradle qui permettent l'import et la consommation des données xml qui seront utilisées pour personnaliser uPortal. Les ressources nécessaires pour la mise en place du portail uPortal sont illustrées dans le tableau suivant :

Fonction	Quantité	CPU	RAM	Espace disque
UPortal	1	2	4Go	30Go

Tableau 1 : Ressources nécessaires pour uPortal

3.6.1.1 Installation de uPortal

Nous avons suivi les étapes d'installation suivantes :

```
./gradlew portalInit
```

L'exécution de cette commande va nous permettre d'effectuer les étapes suivantes :

- Démarre l'instance HSQLDB intégrée : hsqlStart
- Télécharge, installe et configure le conteneur de servlet Tomcat intégré : tomcatInstall.
Le serveur Tomcat n'est pas exécuté dans cette étape. Des instructions pour le démarrer seront présentées ultérieurement.
- Déploie toutes les applications Web d'uPortal sur Tomcat :tomcatDeploy
- Crée le schéma de base de données et importe les ensembles de données Base et Implémentation : dataInit

On peut réexécuter cette commande « ./gradlew portalInit » pour réinitialiser l'environnement à un état propre. En assurant que Tomcat container et l'instance HSQLDB ne sont pas en cours d'exécution.

3.6.1.2 Tomcat

Apache Tomcat est un outil de serveur Web open source développé par Apache Software Foundation (ASF). Il s'agit de l'un des nombreux produits open source liés à Apache utilisés par les professionnels de l'informatique pour diverses tâches et objectifs.¹⁴

Plusieurs étapes de configuration de Tomcat doivent être effectuées pour que le logiciel d'application uPortal fonctionne correctement, cependant uPortal-start est pré-intégré avec le conteneur de servlet Apache Tomcat, qui est requis pour l'exécution de uPortal ainsi de gérer les tâches de configuration, néanmoins on peut télécharger, installer et configurer Tomcat Container à partir de Maven Central, notre choix c'est porté sur uPortal-start (contraintes de temps de réalisation de ce projet)

Démarrage de Tomcat :

```
./gradlew tomcatStart
```

Arrêt de Tomcat :

```
./gradlew tomcatStop
```

Accès à uPoral :

L'url pour accéder à uPortal : <https://uPortal.fsei.com/uPortal>

3.6.2 Zimbra

Tout d'abord, nous avons estimé les ressources nécessaires pour la mise en place d'un serveur Zimbra. Les résultats obtenus sont dans le tableau suivant :

Fonction	Quantité	CPU	RAM	Espace Disque
Ldap-master	1	2	4Go	30Go
Ldap-replica	1	2	4Go	30Go
Logger	1	2	2Go	50Go
Mail store	2	4	8Go	A définir*
Ha proxy	2	2	2Go	30Go

Tableau 2 : Ressources nécessaires pour Zimbra

*L'espace de stockage doit être calculé en fonction du nombre d'étudiants, nombre de documents traités et de la rétention mise en place.

Une fois les spécifications définies, nous sommes passés à l'étape suivante qui consiste en la création de la machine dont l'IP est 192.168.5.133

3.6.2.1 Configuration réseau

Attribution du nom d'hôte zimbra.fsei.com

```
amina@zimbra:~$ cat /etc/hosts
127.0.0.1 localhost
192.168.5.133 zimbra.fsei.com zimbra
192.168.5.134 auth.fsei.com
192.168.5.131 nxcloud.fsei.com
```

Figure 11 : Nom d'hôte

Résultat de la commande `hostname -f`, cette commande retourne le FQDN (full qualified domain name) de la machine.

```
amina@zimbra:~$ hostname -f
zimbra.fsei.com
amina@zimbra:~$
```

Figure 12 : Résultat du FQDN

Création des entrées DNS nécessaires pour le bon fonctionnement du serveur mail

- Création de l'entrée de type A

```

amina@zimbra:~$ dig -t A zimbra.fsei.com

; <<>> DiG 9.10.3-P4-Ubuntu <<>> -t A zimbra.fsei.com
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 33239
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 1280
;; QUESTION SECTION:
;zimbra.fsei.com.                IN      A

;; ANSWER SECTION:
zimbra.fsei.com.                0       IN      A      127.0.0.1

;; Query time: 0 msec
;; SERVER: 127.0.0.1#53(127.0.0.1)
;; WHEN: Thu May 31 20:10:49 CEST 2018
;; MSG SIZE rcvd: 60

```

Figure 13 : configuration DNS (entrée de type A)

- Création de l'entrée de type MX sur le serveur DNS

```

amina@zimbra:~$ dig -t MX zimbra.fsei.com

; <<>> DiG 9.10.3-P4-Ubuntu <<>> -t MX zimbra.fsei.com
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 44980
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
;; QUESTION SECTION:
;zimbra.fsei.com.                IN      MX

;; ANSWER SECTION:
zimbra.fsei.com.                3600   IN      MX     10 zimbra.fsei.com.

;; Query time: 0 msec
;; SERVER: 192.168.5.1#53(192.168.5.1)
;; WHEN: Thu May 31 20:12:27 CEST 2018
;; MSG SIZE rcvd: 60

```

Figure 12 : configuration DNS entré type MX

3.6.2.2 Installation de Zimbra

Récupération du paquet d'installation de Zimbra téléchargement de la version 8 de Zimbra

Lancement du script ¹⁵(install.sh)

```
root@mail:/usr/src/zimbra/zcs-8.8.8_GA_2009.UBUNTU16_64.20180322150747# ./install.sh
Operations logged to /tmp/install.log.9QMaqcFV
Checking for existing installation...
zimbra-chat...NOT FOUND
zimbra-drive...NOT FOUND
zimbra-imapd...NOT FOUND
zimbra-license-tools...NOT FOUND
zimbra-license-extension...NOT FOUND
zimbra-network-store...NOT FOUND
zimbra-network-modules-ng...NOT FOUND
zimbra-ldap...NOT FOUND
zimbra-logger...NOT FOUND
zimbra-mta...NOT FOUND
zimbra-dnscache...NOT FOUND
zimbra-snmp...NOT FOUND
zimbra-store...NOT FOUND
zimbra-apache...NOT FOUND
zimbra-spell...NOT FOUND
zimbra-convert...NOT FOUND
zimbra-memcached...NOT FOUND
zimbra-proxy...NOT FOUND
zimbra-archiving...NOT FOUND
zimbra-core...NOT FOUND
```

Figure 14 : Résultat de install.sh

```
root@mail: /usr/src/zimbra/zcs-8.8.8_GA_2009.UBUNTU16_64.20180322150747
Configuring SNMP...done.
Setting up syslog.conf...done.
Starting servers...done.
Installing common zimlets...
  com_zimbra_clientuploader...done.
  com_zimbra_email...done.
  com_zimbra_ymemoticons...done.
  com_zimbra_srchhighlighter...done.
  com_zimbra_bulkprovision...done.
  com_zimbra_attachmail...done.
  com_zimbra_proxy_config...done.
  com_zimbra_tooltip...done.
  com_zimbra_url...done.
  com_zimbra_cert_manager...done.
  com_zimbra_mailarchive...done.
  com_zimbra_viewmail...done.
  com_zimbra_date...done.
  com_zimbra_attachcontacts...done.
  com_zimbra_adminversioncheck...done.
  com_zimbra_webex...done.
  com_zimbra_phone...done.
Finished installing common zimlets.
Restarting mailboxd...done.
Creating galsync account for default domain...done.
```

Figure 15 : Installation des Zimlets


```
root@mail: /usr/src/zimbra/zcs-8.8.8_GA_2009.UBUNTU16_64.20180322150747
Main menu
  1) Common Configuration:
  2) zimbra-ldap:          Enabled
  3) zimbra-logger:       Enabled
  4) zimbra-mta:          Enabled
  5) zimbra-dnscache:     Enabled
  6) zimbra-snmp:         Enabled
  7) zimbra-store:        Enabled
  8) zimbra-spell:        Enabled
  9) zimbra-proxy:        Enabled
10) Default Class of Service Configuration:
    s) Save config to file
    x) Expand menu
    q) Quit

*** CONFIGURATION COMPLETE - press 'a' to apply
Select from menu, or press 'a' to apply config (? - help) a
Save configuration data to a file? [Yes] y
Save config in file: [/opt/zimbra/config.15367] /opt/zimbra/config.15367
Saving config in /opt/zimbra/config.15367...done.
The system will be modified - continue? [No] y
Operations logged to /tmp/zmsetup.20180413-040510.log
```

Figure 16 : Fin de l'installation de Zimbra

Fin du script

3.6.2.3 Lancement de Zimbra

Comme Zimbra a été liée à un serveur CAS offert par uPortal, nous serons redirigés vers <https://auth.fsei.com> pour s'authentifier et s'identifier par le service CAS qui en retour va envoyer une information du nom de l'utilisateur en utilisant un ticket, une fois l'authentification faite, nous aurons accès à notre messagerie et aussi à l'ENT uPortal.

L'url pour accéder à Zimbra : <https://zimbra.fsei.com>

3.6.2.4 Casification de Zimbra

Cette opération consiste en la délégation de l'identification et l'authentification au serveur CAS. Tout d'abord, il faut importer les certificats du serveur CAS dans le keystore¹⁶ de Zimbra en exécutant la commande suivante :

```
/opt/zimbra/common/bin/keytool -import -file /tmp/cert.pem -alias cascert -trustcacerts
-keystore /opt/zimbra/common/lib/jvm/java/jre/lib/security/cacerts -storepass changeit
```

La seconde opération est l'import de la librairie Java CAS Client dans l'environnement Zimbra, cette opération se fait en exécutant les actions suivantes¹⁷:

- Récupération de la librairie à partir du site officiel de Jasig¹⁸
- La copier de l'archive cas-client-core-3.1.1.jar dans le dossier « /opt/zimbra/jetty/common/lib/ »

Une fois la librairie en place, il faut modifier le fichier de configuration « /opt/zimbra/jetty/etc/zimbra.web.xml.in » afin d'intégrer le système CAS à Zimbra en ajoutant le bloc suivant :

```
<filter>
  <filter-name>CasSingleSignOutFilter</filter-name>
  <filter-class>org.jasig.cas.client.session.SingleSignOutFilter</filter-class>
</filter>

<filter-mapping>
  <filter-name>CasSingleSignOutFilter</filter-name>
  <url-pattern>/*</url-pattern>
</filter-mapping>

<listener>
  <listener-
class>org.jasig.cas.client.session.SingleSignOutHttpSessionListener</listener-class>
</listener>

<filter>
  <filter-name>CasAuthenticationFilter</filter-name>
  <filter-class>org.jasig.cas.client.authentication.AuthenticationFilter</filter-class>
  <init-param>
    <param-name>casServerLoginUrl</param-name>
    <param-value>https://auth.fsei.com:443/cas/login</param-value>
  </init-param>
  <init-param>
    <param-name>serverName</param-name>
    <param-value>https://zimbra.fsei.com:443</param-value>
  </init-param>
</filter>

<filter-mapping>
  <filter-name>CasAuthenticationFilter</filter-name>
  <url-pattern>/public/preauth.jsp</url-pattern>
</filter-mapping>

<filter>
  <filter-name>CasValidationFilter</filter-name>
  <filter-
class>org.jasig.cas.client.validation.Cas20ProxyReceivingTicketValidationFilter</filter-
class>
  <init-param>
    <param-name>casServerUrlPrefix</param-name>
    <param-value>https://auth.fsei.com:443/cas</param-value>
  </init-param>
  <init-param>
    <param-name>serverName</param-name>
    <param-value>https://zimbra.fsei.com:443</param-value>
  </init-param>
  <init-param>
    <param-name>redirectAfterValidation</param-name>
    <param-value>>true</param-value>
  </init-param>
</filter>

<filter-mapping>
  <filter-name>CasValidationFilter</filter-name>
  <url-pattern>/*</url-pattern>
</filter-mapping>

<filter>
  <filter-name>CasHttpServletRequestWrapperFilter</filter-name>
```

```
<filter-class>org.jasig.cas.client.util.HttpServletRequestWrapperFilter</filter-  
class>  
</filter>  
  
<filter-mapping>  
  <filter-name>CasHttpServletRequestWrapperFilter</filter-name>  
  <url-pattern>/*</url-pattern>  
</filter-mapping>
```

Ensuite, nous devons créer une clé qui sera utilisée par le script de pré-authentification de Zimbra. Cette opération se fait en exécutant la commande suivante :

```
zmprov gdpak zimbra.fsei.com
```

Cette clé doit être la valeur de la constante DOMAIN_KEY du fichier « preauth.jsp » qui se trouve « /opt/zimbra/jetty/webapps/zimbra/public/preauth.jsp ».

Pour information, ce fichier peut être récupéré à partir du site officiel de Jasig ou ailleurs.

Finalement, il faut modifier les URL de connexion et de déconnexion utilisées par Zimbra :

```
zmprov md yourdomain.com zimbraWebClientLoginURL  
https://zimbra.fsei.com/public/preauth.jsp  
zmprov md yourdomain.com zimbraWebClientLogoutURL https://auth.fsei.com/cas/logout  
zmprov mcf zimbraWebClientLoginURL https://zimbra.fsei.com/public/preauth.jsp  
zmprov mcf zimbraWebClientLogoutURL https://auth.fsei.com/cas/logout
```

Afin que les différentes modifications soient prises en charge, un redémarrage du service est nécessaire :

```
zmcontrol restart
```

3.6.3 Nextcloud

Nextcloud est un logiciel de cloud collaboratif, libre et open source permet d'héberger ses propres fichiers en mode SaaS (Software as a Service) sans dépendre d'autres intervenants. C'est un outil de partage et de synchronisation de documents simples à mettre en place et à prendre en main avec la limite du stockage qui va dépendre du serveur¹⁹.

Pour installer ce service, il suffit de récupérer l'archive à partir du site officiel de Nextcloud et de la décompresser dans le répertoire racine du serveur web.

Une fois les différents fichiers présents à la racine du répertoire, il faudra compléter l'installation en suivant le guide proposé par Nextcloud via son interface web :

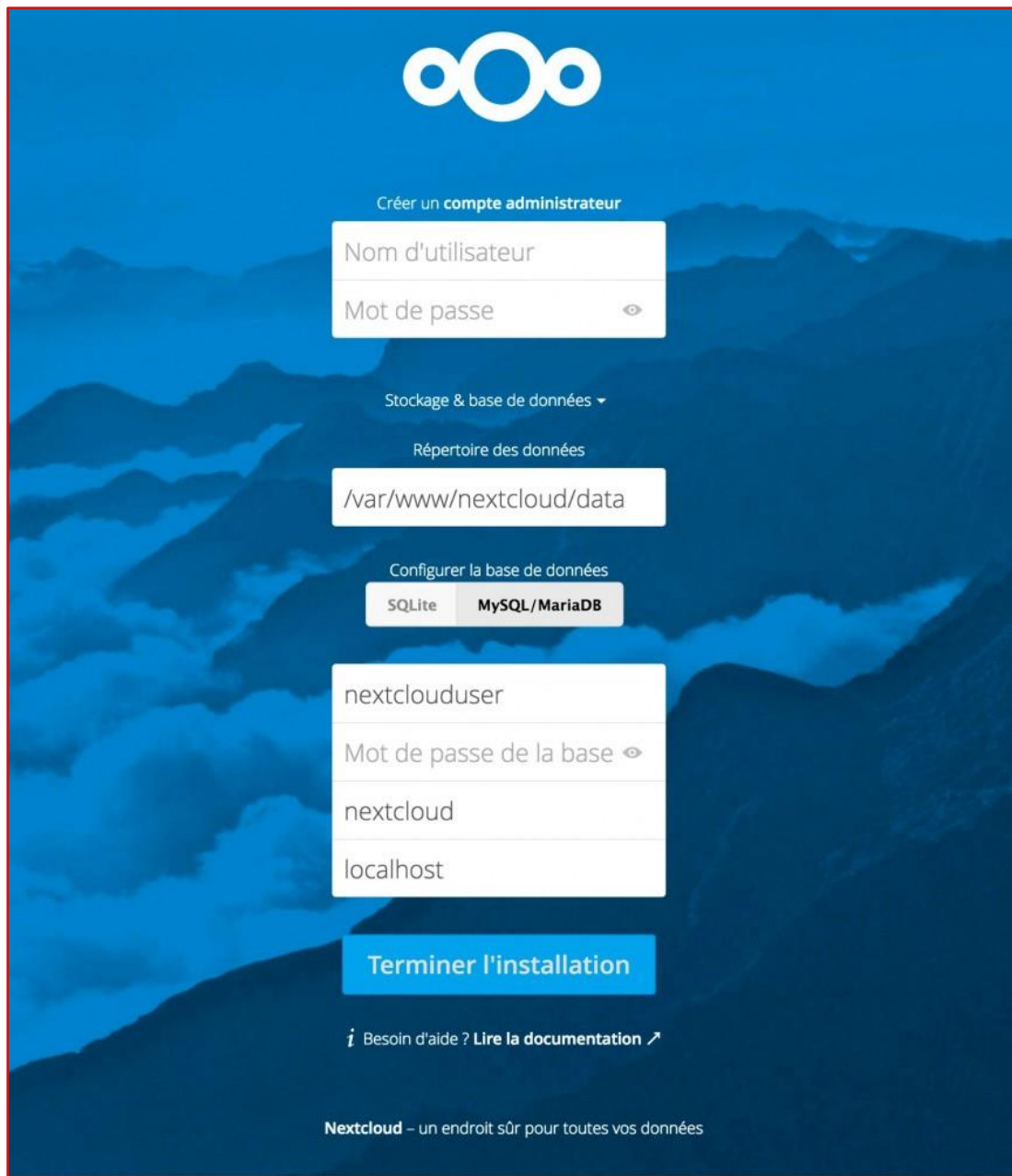


Figure 17 : Interface Web de NEXTCLOUD

Pour configurer les fonctionnalités nécessaires à notre environnement, nous nous sommes basés sur la documentation officielle afin de créer un fichier de configuration correcte :

```
// Contenu du fichier config.php
$CONFIG = array (
  'instanceid' => 'oc90qfu1lews',
  'passwordsalt' => '4GqbWdLM2c0ZUc0BZfdfsfw0FV7P+3g',
  'secret' => 'zMR0aINhto4iFag8MSTo105HFueDjdgJUjLxCM3+WcDfSRum',
  'trusted_domains' =>
  array (
    0 => '192.168.5.131',
    1 => 'nxcloud.fsei.com',
  ),
),
```

```
'datadirectory' => '/var/www/nextcloud/data',
'overwrite.cli.url' => 'https://nxcloud.fsei.com',
'dbtype' => 'mysql',
'version' => '13.0.2.1',
'dbname' => 'nextcloud',
'dbhost' => '127.0.0.1:3306',
'dbport' => '',
'dbtableprefix' => 'oc_',
'dbuser' => 'nextcloud',
'dbpassword' => 'nextcloud',
'installed' => true,
'ldapIgnoreNamingRules' => false,
'ldapProviderFactory' => '\\OCA\User_LDAP\LDAPProviderFactory',
'mail_from_address' => 'admin',
'mail_smtpmode' => 'php',
'mail_smtpauthtype' => 'LOGIN',
'mail_domain' => 'zimbra.fsei.com',
);
```

3.6.3.1 Zimbra et Nextcloud

Nextcloud s'intègre à Zimbra via un zimlet. le zimlet ²⁰doit être installé et configuré sur le serveur Zimbra, ce zimlet utilise le protocole webDAV (web-based Distributed Authoring and Versioning) qui est une extension du http avec les méthodes PUT, DELETE, COPY, PROPFIND) etc... en plus à ceux des GET et POST²¹.

- **Fonctionnalité de Nextcloud :**

- Synchronisation de fichiers entre différents ordinateurs tablettes et smartphone.
- Stockage sécurisé.
- Partage de fichiers entre utilisateurs nextcloud ou utilisateurs externes.
- Serveurs de fichiers WebDAV.
- Calendrier.
- Gestionnaire de contacts.
- Visionnaire de documents en ligne (PDF, openDocument).
- Galerie d'image multi formats (jpg,cr2,img ...).
- Messagerie web expérimentale.
- Antivirus.
- Et de nombreuse application (annoncements ...).

3.7 Le SSO en action

Lorsque nous accédons à une application reliée au SSO pour la première fois, nous aurons accès au contenu non protégé de l'application.

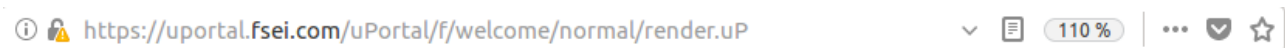


Figure 13 : URL d'accès pour uPortal

La page d'accueil de l'application web sera affichée avec le contenu non protégé.

L'activation d'un lien menant à une ressource protégée tel que le « Sign in » pour avoir accès à l'espace utilisateur (admin, simple user), provoquera au client une redirection par l'application vers le serveur CAS un serviceID ce service est en effet une URL qui va permettre au serveur CAS d'identifier l'application qui à rediriger le client vers le serveur CAS.

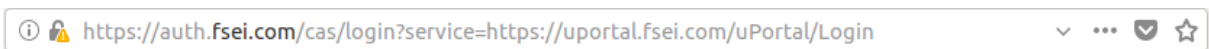


Figure 18 : URL de redirection au serveur CAS

Le serveur CAS affiche alors au client un formulaire d'authentification illustré dans la figure suivante :

Figure 19 : Formulaire d'authentification CAS

Une fois que le client aura réussi à s'authentifier, le serveur CAS va exécuter trois instructions :

- Déposer un cookie de session sécurisée (CASTGC) acronyme qui signifie CAS ticket granting cookie sur le chemin /cas, c'est le cookie sur lequel repose la partie SSO de l'authentification, un cookie de session qui va donc persister jusqu'à la fermeture du navigateur (l'expiration de la session http).

- Générer un service ticket (ST). Il s'agit d'un nombre aléatoire sans signification particulière, le serveur CAS le stocke dans sa mémoire et l'associe à l'identifiant du client. La durée de vie du service ticket est très brève : de l'ordre de quelques secondes.
- Contrôler que le service ID que lui a fourni le client correspond bien à un service qui lui est raccordé, puis rediriger à son tour le client vers l'URL correspondant au service ID, en lui donnant le service ticket en paramètre GET.

L'application récupère le service ticket dans la requête de redirection et appelle directement le serveur CAS en mode M2M en lui donnant le service ticket, ensuite le serveur CAS vérifie que l'URL de l'application est bien enregistrée et contrôle si c'est bien l'URL associée au ticket. Ensuite, l'application attribue le rôle AUTHENTICATED au client, connaissant l'identifiant du client elle va interroger sa base de données pour récupérer les informations de ce client et lui afficher un contenu adapté à son profil.



Figure 20 : Identification du profil après authentification

La figure ci-dessous représente le diagramme de séquence d'une première authentification via CAS :

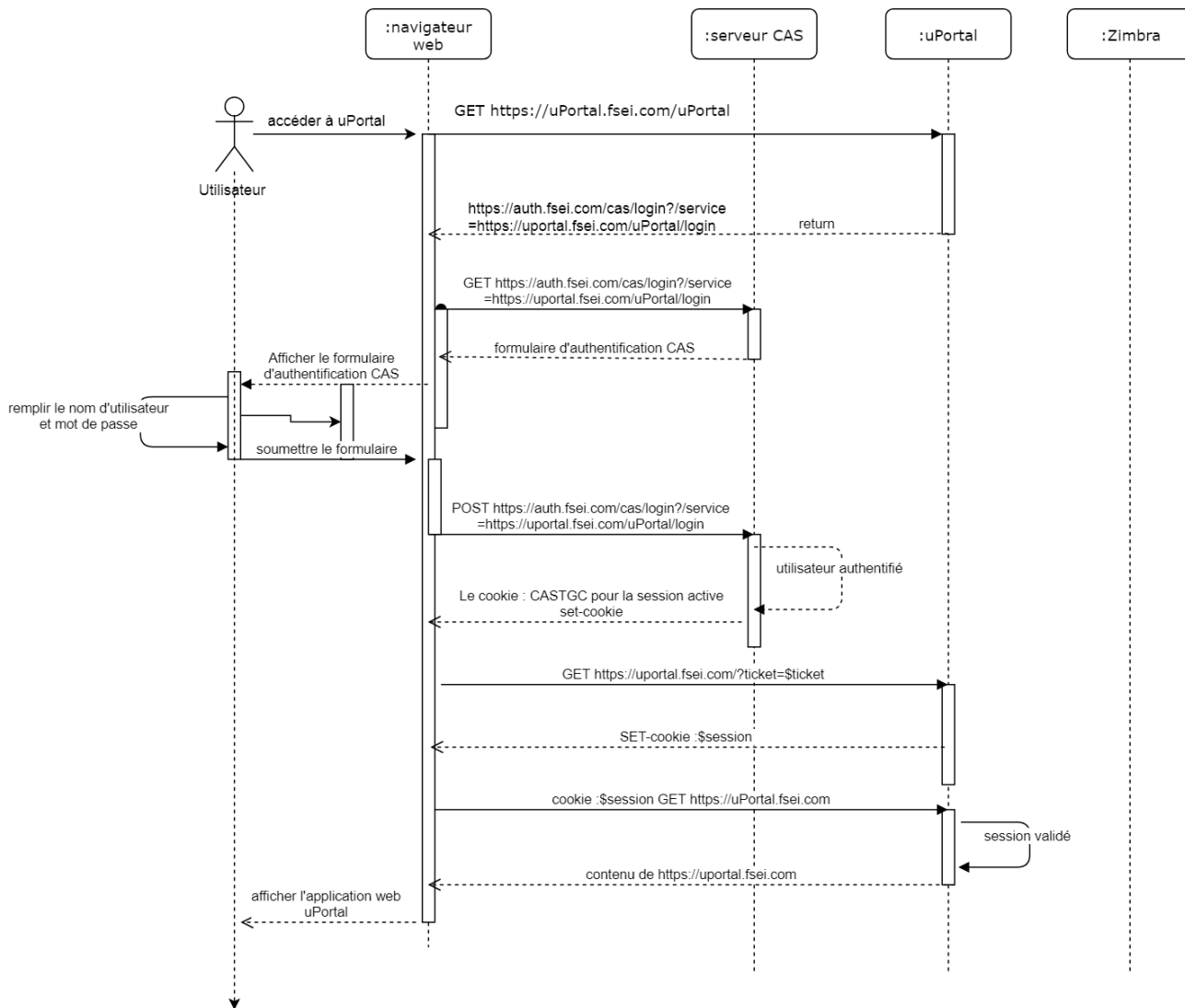


Figure 21 : Diagramme de séquence du premier accès via le SSO CAS

3.7.1 Accès à une seconde application reliée au SSO

Un client authentifié sur une application donnée qui souhaite accéder à une deuxième application, celle-ci va réagir systématiquement de la même manière que la première authentification à savoir :

- Rediriger le client vers le serveur CAS avec le serviceID en paramètre (le client ne se rendra pas compte de cette redirection).

- Le serveur CAS va observer que le client possède un cookie sécurisé CASTGC, si il est valide, le serveur va en extraire l'identifiant de l'utilisateur, et le considère comme déjà authentifié et saute l'étape de l'affichage du formulaire d'authentification ; Ainsi l'utilisateur accédera au contenu protéger de la deuxième application sans avoir eu a rentré à nouveau son login et mot de passe.



Figure 22 : URL d'accès à Zimbra via le SSO

La figure ci-dessous représente le diagramme de séquence d'une deuxième authentification via CAS :

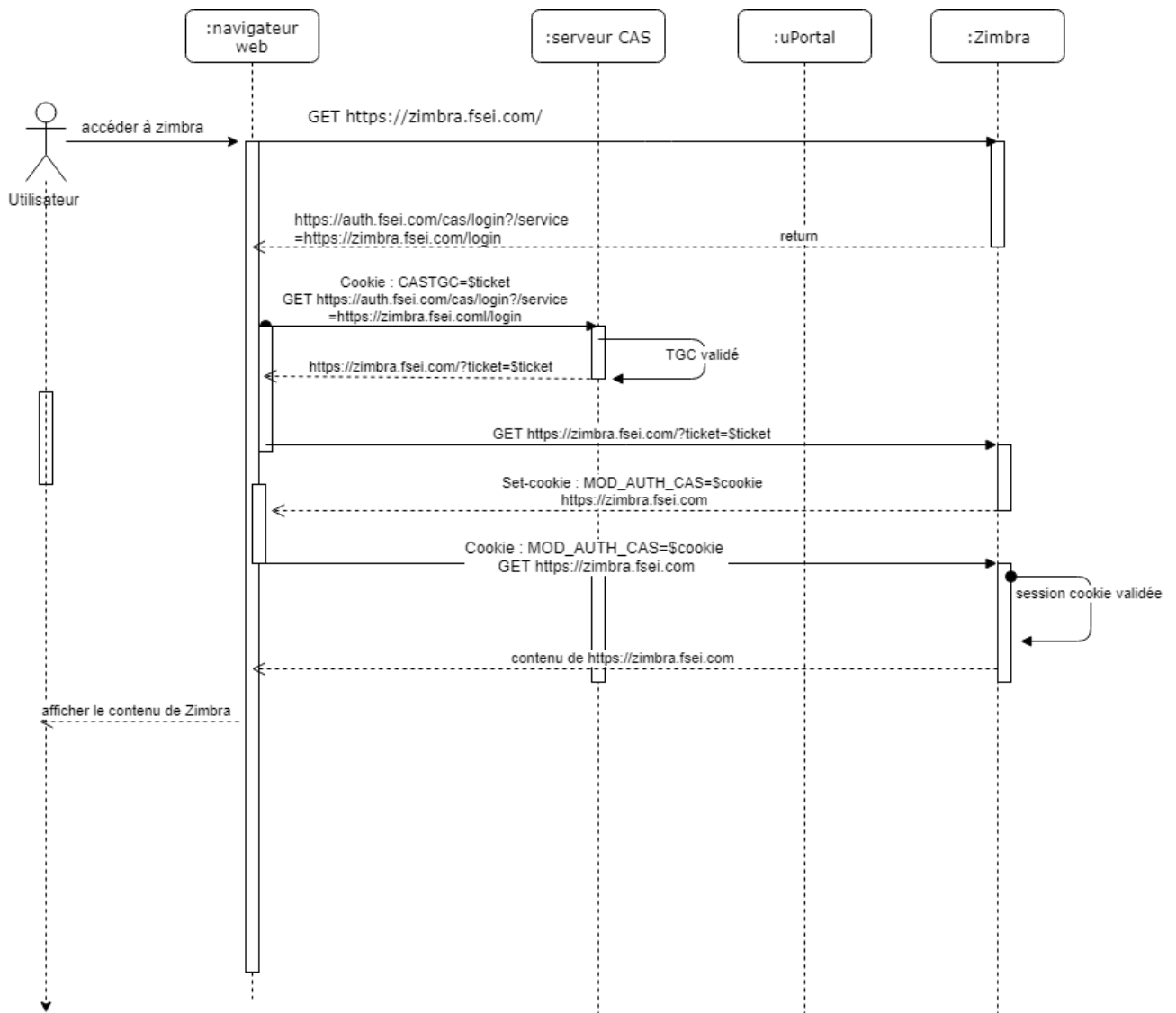


Figure 23 : diagramme de séquence d'accès à la seconde application du SSO

3.7.2 Déconnexion du SSO

Les applications reliées au SSO disposent d'un lien de déconnexion propre à chacune, quand le client se déconnecte de l'une d'entre elles, ceci ne va pas le déconnecter du SSO, mais seulement de l'application choisie.

Mettre fin à son authentification SSO en détruisant le cookie CASTGC, par un appel de L'URL /cas/logout du serveur CAS.



Figure 24 : Appel de L'URL de déconnexion du serveur CAS

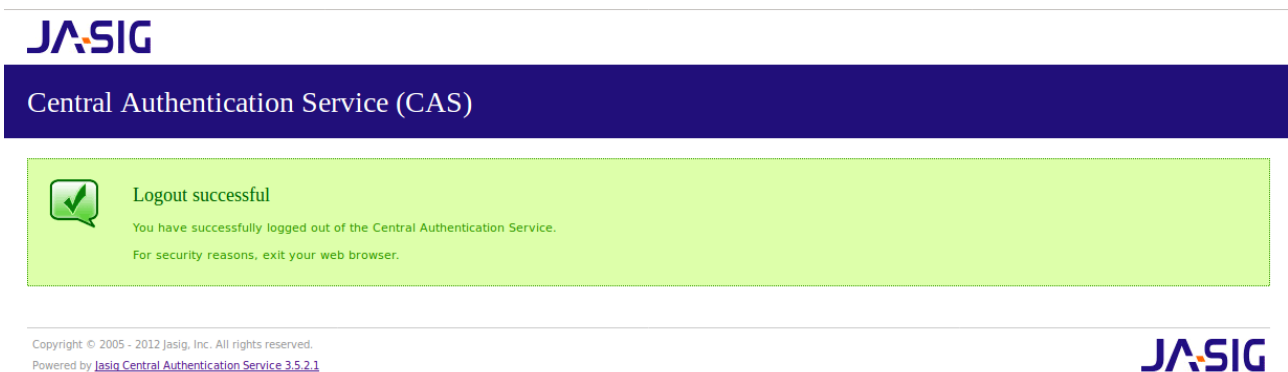


Figure 25 : Déconnexion du serveur CAS

3.8 Administration de uPortal, Zimbra et nextcloud

3.8.1 uPortal

Lorsqu'un utilisateur se connecte sur uPortal via le « sign-in » il aura accès à un contenu et une mise en page personnalisée selon le type de l'utilisateur défini.

3.8.1.1 Types d'utilisateurs disponibles sur uPortal :

- **L'administrateur** : administrer de nombreux aspects du portail, notamment la publication de nouveaux contenus et la modification du contrôle d'accès.
- **L'étudiant** : accès aux différents contenus qui lui ont été accordés par l'administrateur, avec un espace personnalisable
- **Le développeur** : disposant de à peu près le même droit qu'un administrateur, mais avec un plus sur le côté développement notamment la configuration des portlets.
- **Faculté et personnels** : tout simplement le contenu de la faculté qui ne sera pas d'une grande différence à celui d'un étudiant, mis à part le contenu attribué.

3.8.1.2 Interfaces utilisateurs :

Après s'être authentifié auprès du serveur CAS pour accéder à uPortal autant qu'étudiant :
L'utilisateur peut customiser son interface selon son choix et priorité.

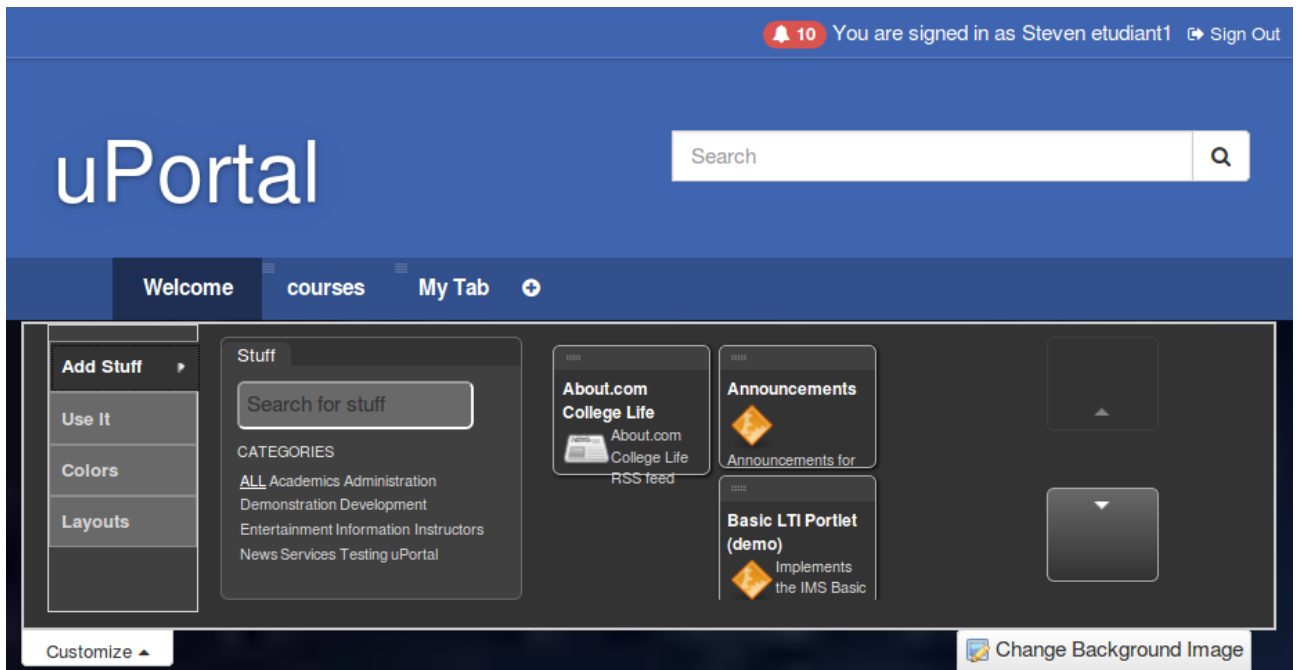


Figure 26 : Interface utilisateur uPortal

L'accès au compte Zimbra de l'utilisateur via l'interface de uPortal :

Via la portlet Email qui est préalablement installé sur uPortal, qui donnera un aperçu de l'état de la boîte mail de l'utilisateur



Figure 27 : Portlet Email de Zimbra

3.8.1.3 Portlet Courses :

C'est une portlet qui regroupe la liste de cours auxquels l'étudiant assiste du moins qu'il aura choisi d'ajouter à cette liste privée.

Cette portlet peut être configuré par la suite pour par exemple :

- Relier les cours auxquels l'étudiant dispose dans son emploi du temps avec la liste des cours.
- Être informé d'un changement quelconque concernant un des cours de la liste
- Changement de l'emploi du temps ou toutes autres informations susceptibles de le concerner

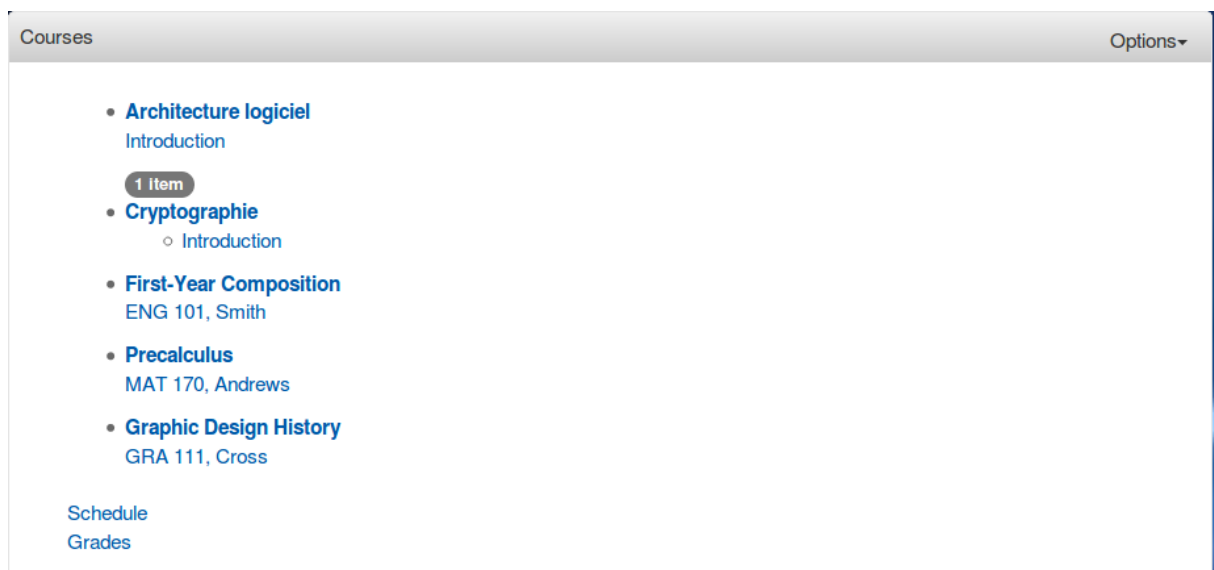


Figure 28 : Portlet courses de uPortal

3.8.1.4 Interface administrateur

L'interface administrateur diffère de celle des autres utilisateurs, du fait qu'elle donne accès aux outils administratifs.

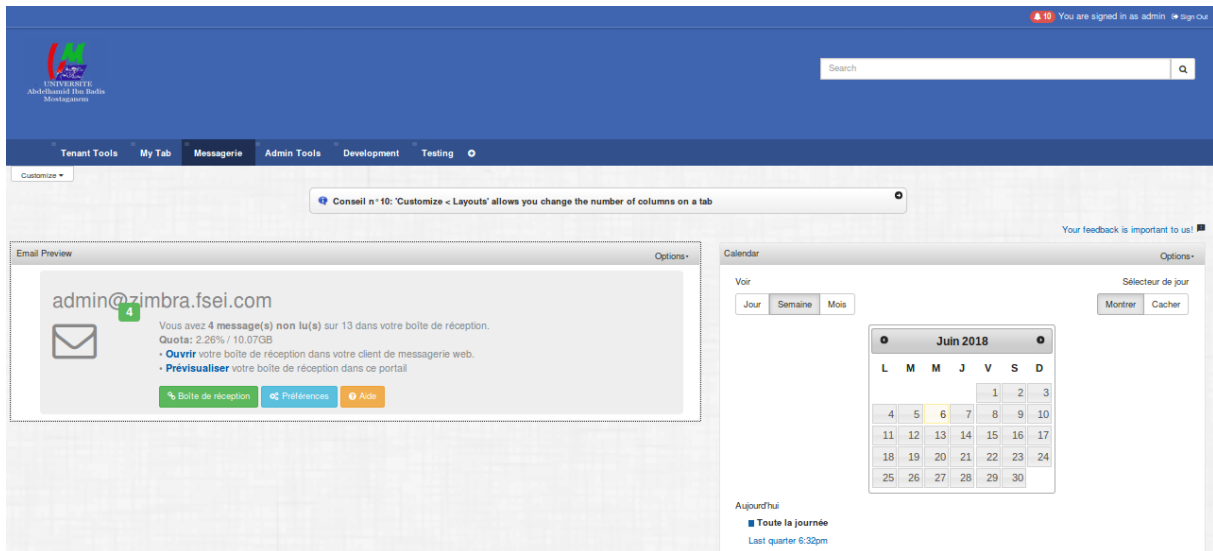


Figure 29 : Interface administrateur uPortal

Outils administratifs qui feront objet d'administrer le portail web notamment :

- Administration des utilisateurs.
- Gestion des permissions et droits d'accès des utilisateurs.
- Gestion administrative des portlets.
- Importation, exportation (portlet, users).
- Gestion des annonces administrative.

Et d'autres outils qui seront illustrés dans la figure ci-dessous

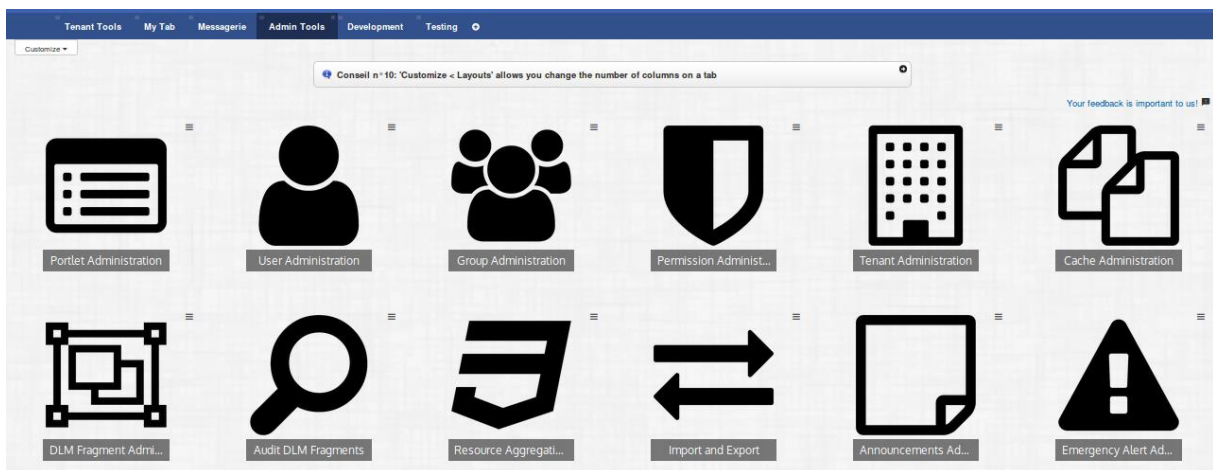


Figure 30 : Outils d'administration uPortal

3.8.2 Administration de Zimbra

3.8.2.1 Administration de serveur de messagerie :

L'administration de Zimbra peut se faire de deux manières :

- Via l'interface graphique avec un simple navigateur web
- En ligne de commande avec un émulateur de terminal

La liste des CLI (commande line interface) de Zimbra :

CLI	Descriptions
Ldap	Start ,stop ou status de zimbra LDAP
Ldap search	La recherche dans le serveur LDAP
Mailboxd	Start, stop, status du serveur mailboxd
Mysql,server	Start, stop l'instance SQL pour le package mailbox
Zmaccts	Listes des comptes, status des comptes/domaine
Zmantispamctl	Start,stop, reload, status du service anti spam
Zmantivirusctl	Start,stop, reload, status du service anti virus
Zmcalchk	Vérifier la cohérence des rendez-vous et des participants dans le calendrier Zimbra
zmcontrol (Start/Stop Service)	Start, stop, status du serveur Zimbra. Et pour trouver la version installée de Zimbra
zmdumpenv	Des informations générales sur l'environnement du serveur sont affichées
zmldappasswd	Change le mot de passe du LDAP
zmlocalconfig	Utilisé pour définir ou obtenir la configuration locale d'un serveur Zimbra
zmloggerctl	Start, stop, reload, status du service Zimbra logger
zmloggerhostmap	Utilisé pour mapper manuellement un nom d'hôte DNS à un zmhostname
zmmailbox	Effectue des tâches de gestion de mailbox
zmprov (Provisioning)	Effectue toutes les tâches de provisioning dans ZAP, y compris la création de comptes, de domaines, de listes de distribution et d'alias
Zmpython	Possibilité d'écrire des scripts Python qui accèdent aux bibliothèques Java Zimbra. Il définit le chemin de la classe ZCS et lance l'interpréteur Jython.

Tableau 3 : Commande line interface

- Les CLI se trouve dans le dossier /opt/zimbra/bin
- Le dossier contenant les messages : /opt/zimbra/store

- Le dossier Mysql contenant les bases de données est opt/zimbra/db
- Le dossier contenant le logs : /opt/zimbra/log

3.8.2.2 Console d'administration

On accède à la console d'administration via l'URL :



Figure 31 : URL de la console d'administration Zimbra

Ensuite on va s'identifier en tant qu'Admin avec le mot de passe déjà attribué au cours de l'installation de Zimbra comme le montre la figure ci-dessous :

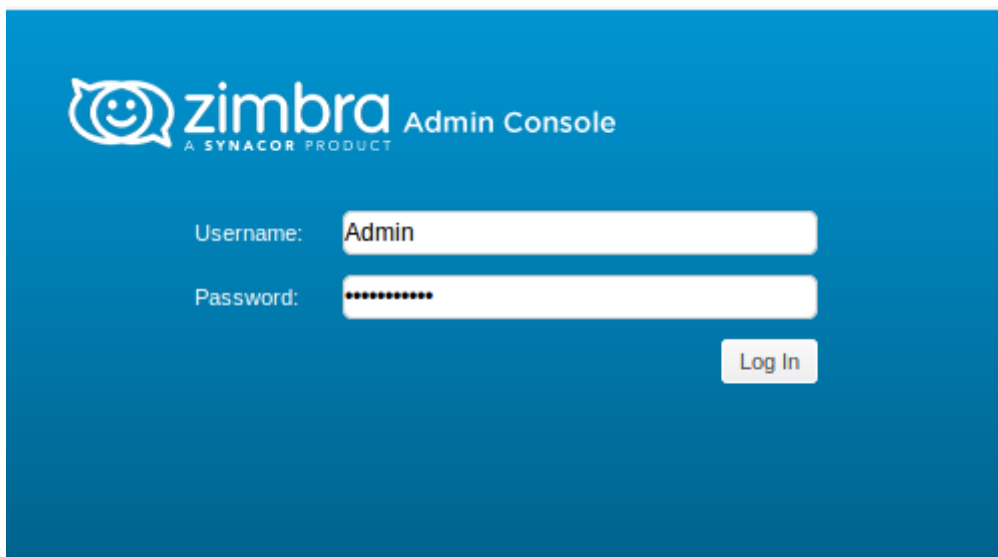


Figure 32 : Interface web administrateur

Création des comptes utilisateurs :

Pour créer des comptes utilisateurs on va accéder à l'espace dédié pour « comptes »

Home →manage → accounts → new

Ensuite on doit renseigner les champs obligatoires à la création du compte c'est-à-dire, le nom du compte et le nom de l'utilisateur, toute autre information peut être ajoutée, modifiée et supprimée après la création du compte.

Le mot de passe peut ne pas être attribué à cette étape de création dans le cas d'une authentification externe, dans le cas contraire (attribution de mot de passe) cela ne va pas influencer sur l'authentification.

La figure suivante montre l'interface de création d'un compte Zimbra :

The screenshot shows the 'New Account' window with the 'General Information' tab selected. The 'Account Name' section contains the following fields: 'Account name:*' with 'etudiant' and '@ zimbra.fsei.com', 'First name:' with 'amina', 'Middle initial:', 'Last name:*' with 'benmekki', and 'Display name:' with 'amina benmekki' and a checked 'auto' checkbox. Below this is an unchecked 'Hide in GAL' checkbox. The 'Account Setup' section has a 'Status:' dropdown menu set to 'Active'. At the bottom, there are 'Help', 'Cancel', 'Previous', 'Next', and 'Finish' buttons.

Figure 33 : Informations générales du compte

3.8.2.3 Aliases

On peut également définir des alias pour des adresses mail :

The dialog box is titled 'Define email aliases for the new account.' It features a text input field for the alias, followed by an '@' symbol and another text input field for the domain. Below the first input field is an 'Add alias' button, and to the right of the domain input field is a 'Remove' button.

Figure 34 : Aliases

3.8.2.4 Caractéristiques

Dans cette partie de configuration du compte on peut attribuer des caractéristiques spécifiques à chaque compte comme le montre la figure suivante :

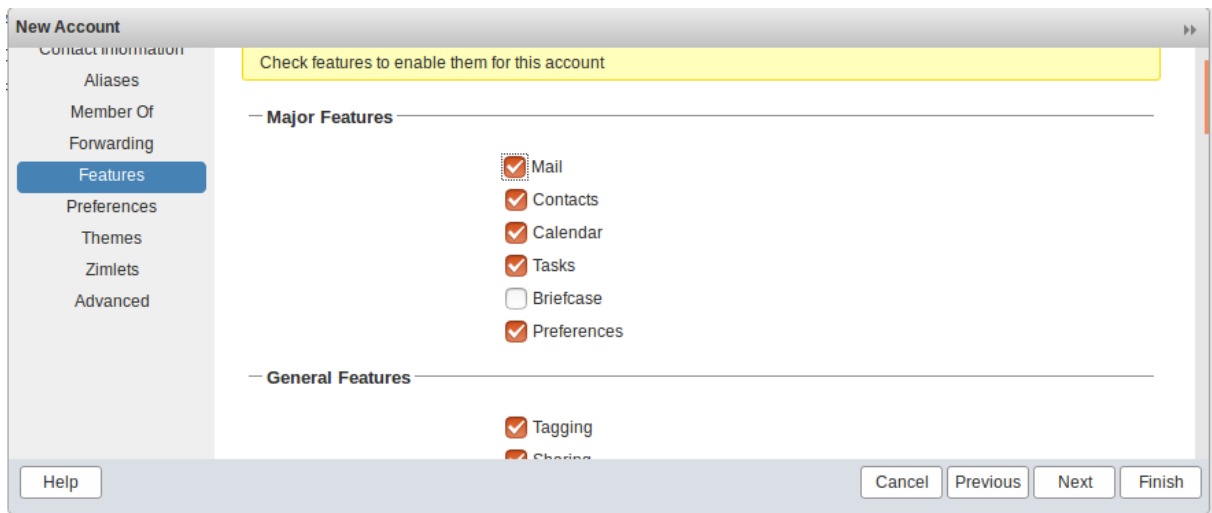


Figure 35 : caractéristiques du compte créé

3.8.2.5 Liste des comptes créés

La figure ci-dessous illustre les comptes utilisés pour les tests

Email Address	Display Name	Status	Last Login Time	Description
admin@zimbra.fsei.com		Active	30 May, 2018 02:05:22	Administrative Account
enseignant1@zimbra.fsei.com	enseignant1	Active	8 May, 2018 14:33:52	
enseignant2@zimbra.fsei.com	enseignant2	Active	Never logged in	
enseignant3@zimbra.fsei.com	enseignant3	Active	Never logged in	
enseignant4@zimbra.fsei.com	enseignant4	Active	Never logged in	
enseignant5@zimbra.fsei.com	enseignant5	Active	Never logged in	
enseignant6@zimbra.fsei.com	enseignant6	Active	Never logged in	
enseignant7@zimbra.fsei.com	enseignant7	Active	Never logged in	
etudiant10@zimbra.fsei.com	etudiant10	Active	Never logged in	
etudiant11@zimbra.fsei.com	etudiant11	Active	Never logged in	
etudiant12@zimbra.fsei.com	etudiant12	Active	Never logged in	
etudiant13@zimbra.fsei.com	etudiant13	Active	Never logged in	
etudiant1@zimbra.fsei.com	etudiant1	Active	26 May, 2018 01:24:23	
etudiant2@zimbra.fsei.com	etudiant2	Active	9 May, 2018 13:12:57	
etudiant3@zimbra.fsei.com	etudiant3	Active	27 May, 2018 13:22:50	
etudiant4@zimbra.fsei.com	etudiant4	Active	30 May, 2018 02:50:50	
etudiant5@zimbra.fsei.com	etudiant5	Active	Never logged in	
etudiant6@zimbra.fsei.com	etudiant6	Active	Never logged in	
etudiant7@zimbra.fsei.com	etudiant7	Active	Never logged in	
etudiant8@zimbra.fsei.com	etudiant8	Active	Never logged in	
etudiant9@zimbra.fsei.com	etudiant9	Active	Never logged in	

Figure 36 : liste des comptes Zimbra

3.8.2.6 Accès utilisateur

La console utilisateur de Zimbra de base est représenté comme suit :

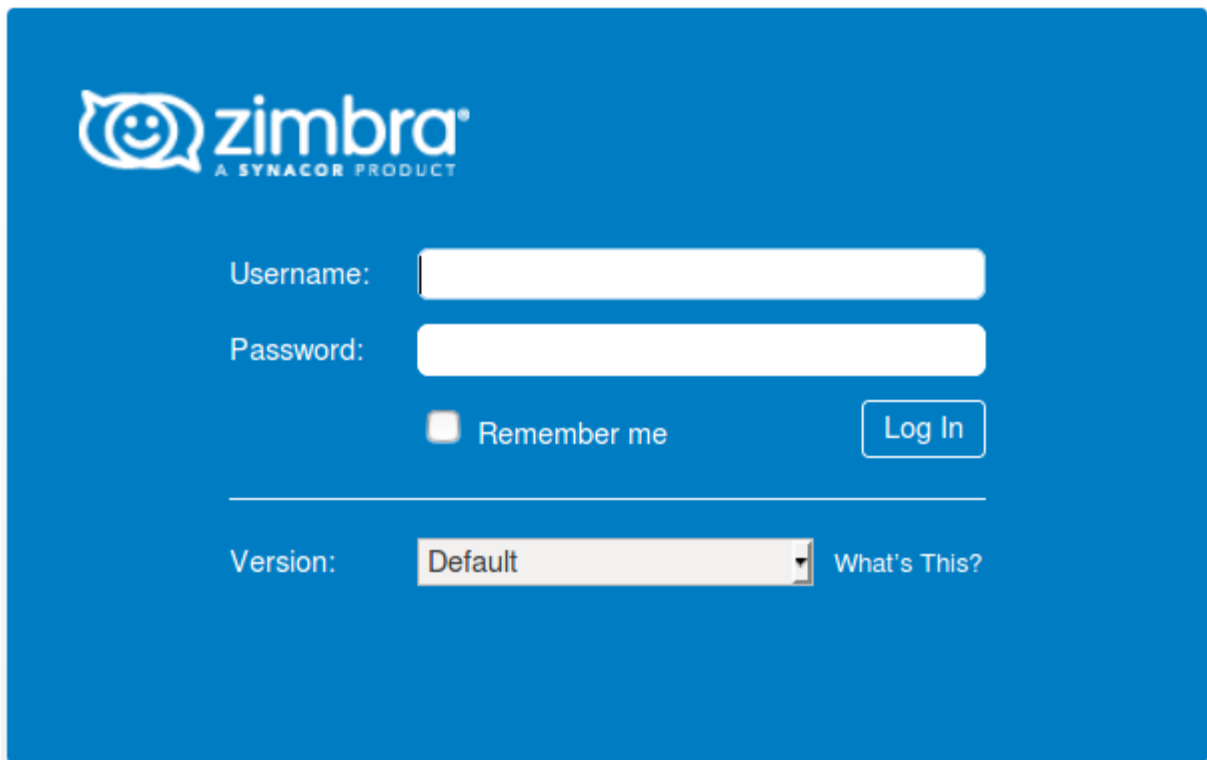


Figure 37 : Interface utilisateur Zimbra

Elle va être remplacée par l'interface d'authentification offerte par le serveur CAS.

Cependant, l'application Zimbra a été casifiée par le serveur CAS, ce qui explique l'interface d'authentification CAS quand on veut accéder aux comptes de Zimbra ce qui va donner une interface web totalement différente.



Figure 38 : Interface d'authentification de Zimbra

Après s'être authentifié auprès du serveur CAS (comme expliqué précédemment sur l'authentification SSO CAS), on aura accès à la page d'accueil de la messagerie, dont on montre l'aperçu.

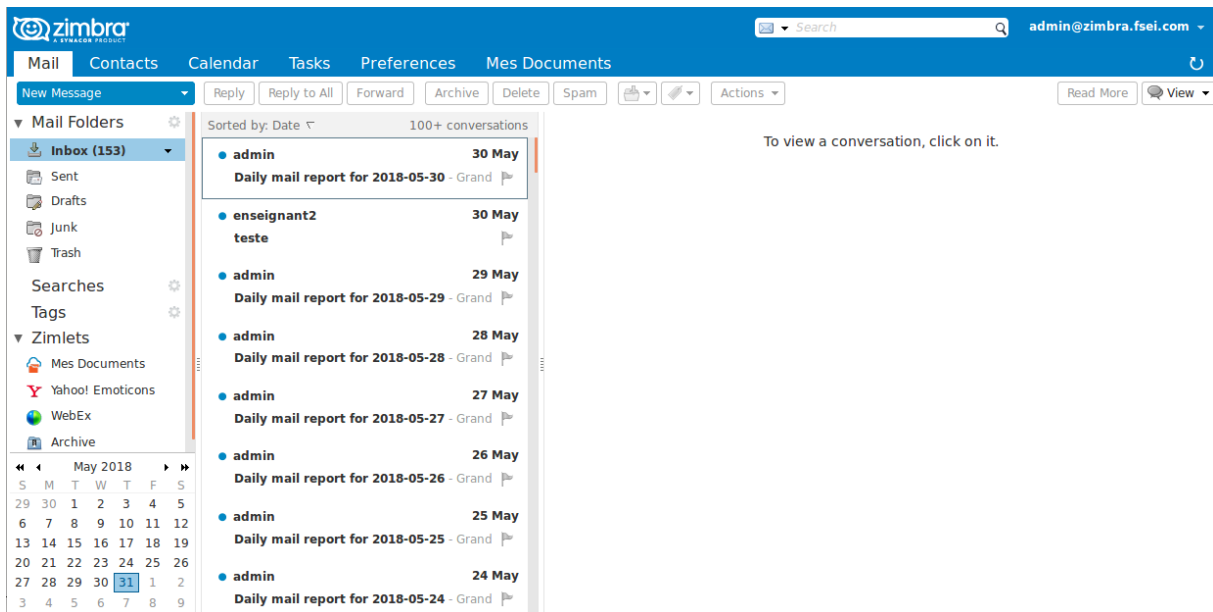


Figure 39 : Page d'accueil d'un compte Zimbra

3.8.3 Nextcloud

L'accès à nextcloud via l'interface utilisateur du compte Zimbra après avoir ajouté le Zimlet de nextcloud, une rubrique « mes documents » est ajoutée qui va permettre à l'utilisateur d'avoir accès à son espace cloud, de consulter et d'ajouter des fichiers au compte nextcloud.

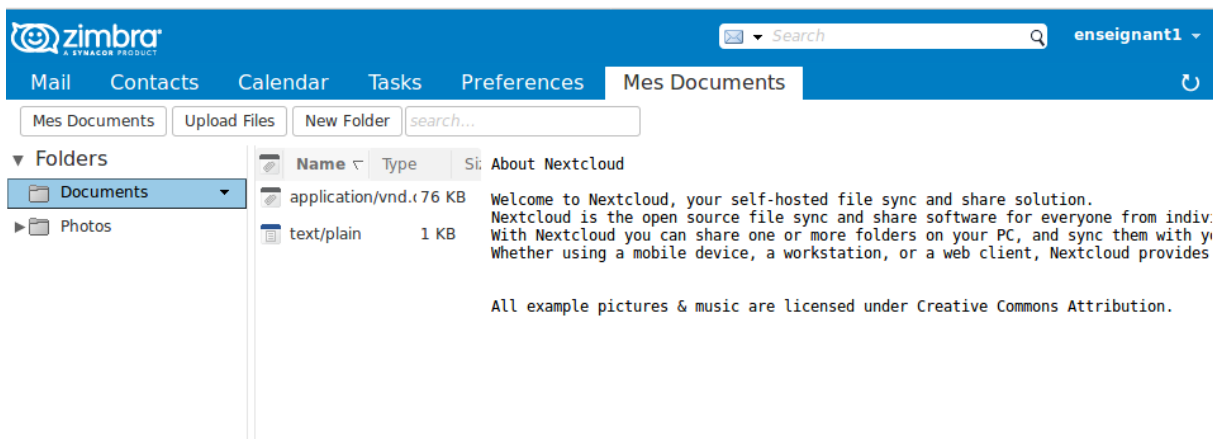


Figure 40 : Accès à nextcloud via Zimbra

Pour accéder à l'espace de nextcloud on peut le faire via le lien <https://nxtcloud.fsei.com> ou directement en cliquant sur « Mes documents » dans l'interface Zimbra.

Une page d'authentification est chargée comme le montre la figure suivante :

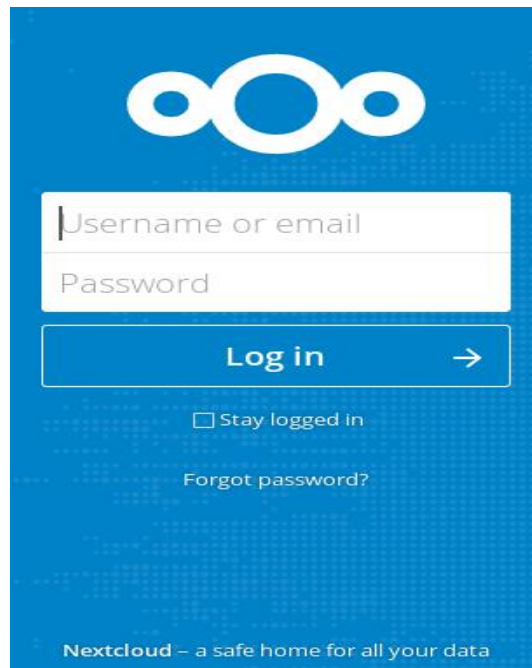


Figure 41 : Interface d'authentification nextcloud

Après s'être authentifié on aura accès à l'espace « files » où on peut trouver tous nos documents ajoutés soit par nous-même ou qui ont été partagés « shared with you », ou ceux que nous même nous avons partagés avec un utilisateur ou un groupe d'utilisateurs avec « shared with others » .

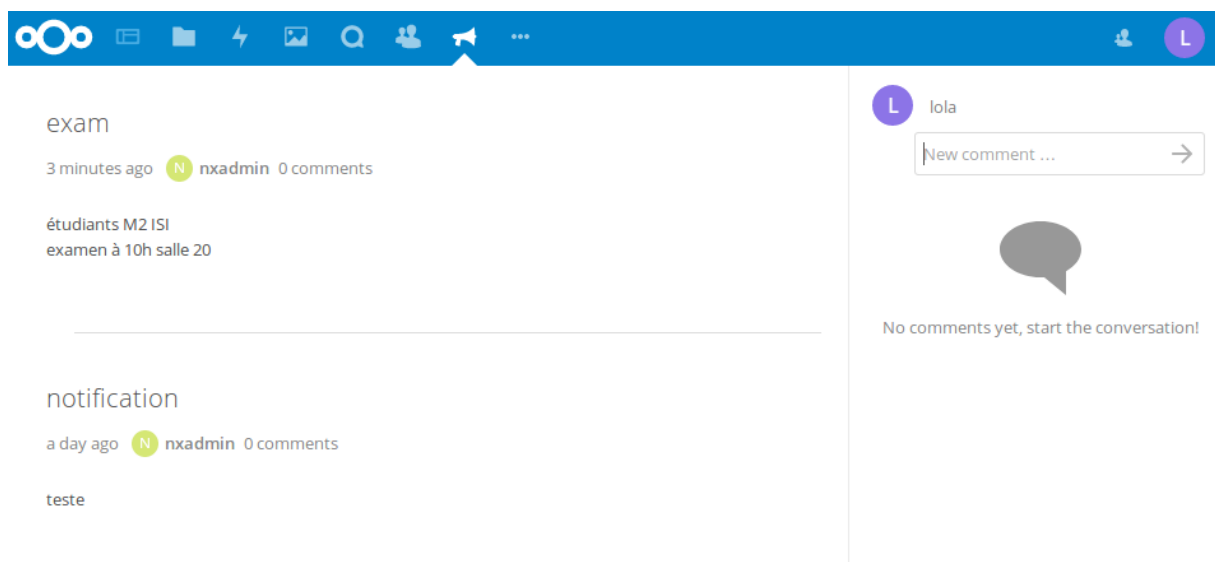


Figure 42 : Espace de partage de fichiers sous nextcloud

L'utilisateur va disposer d'un espace où on y trouve les informations personnelles qui peuvent être privées ou visibles aux public/contacts tel que la photo de profil, l'email, l'adresse, numéro de téléphone, site web et les groupes auxquels il appartient.

La figure suivante illustre la partie personnelle de l'utilisateur Nextcloud qui se trouve dans la rubrique paramètres.

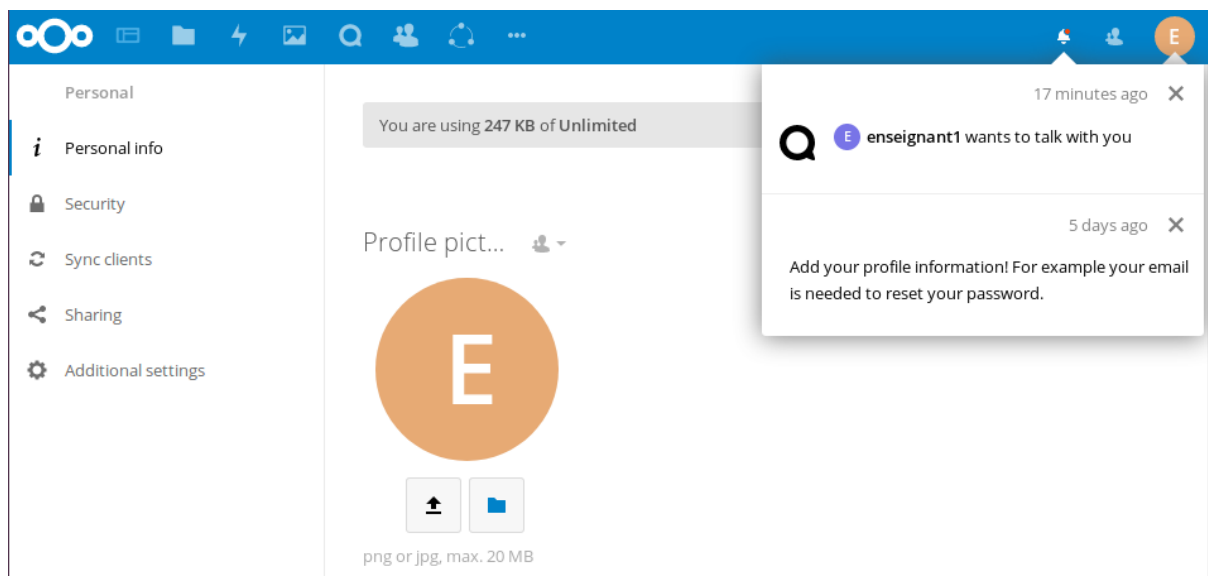


Figure 43 : Informations personnelles sous nextcloud

3.8.3.1 Administration de Nextcloud

Gestions des utilisateurs et des groupes, la figure illustre le principe de gestion :

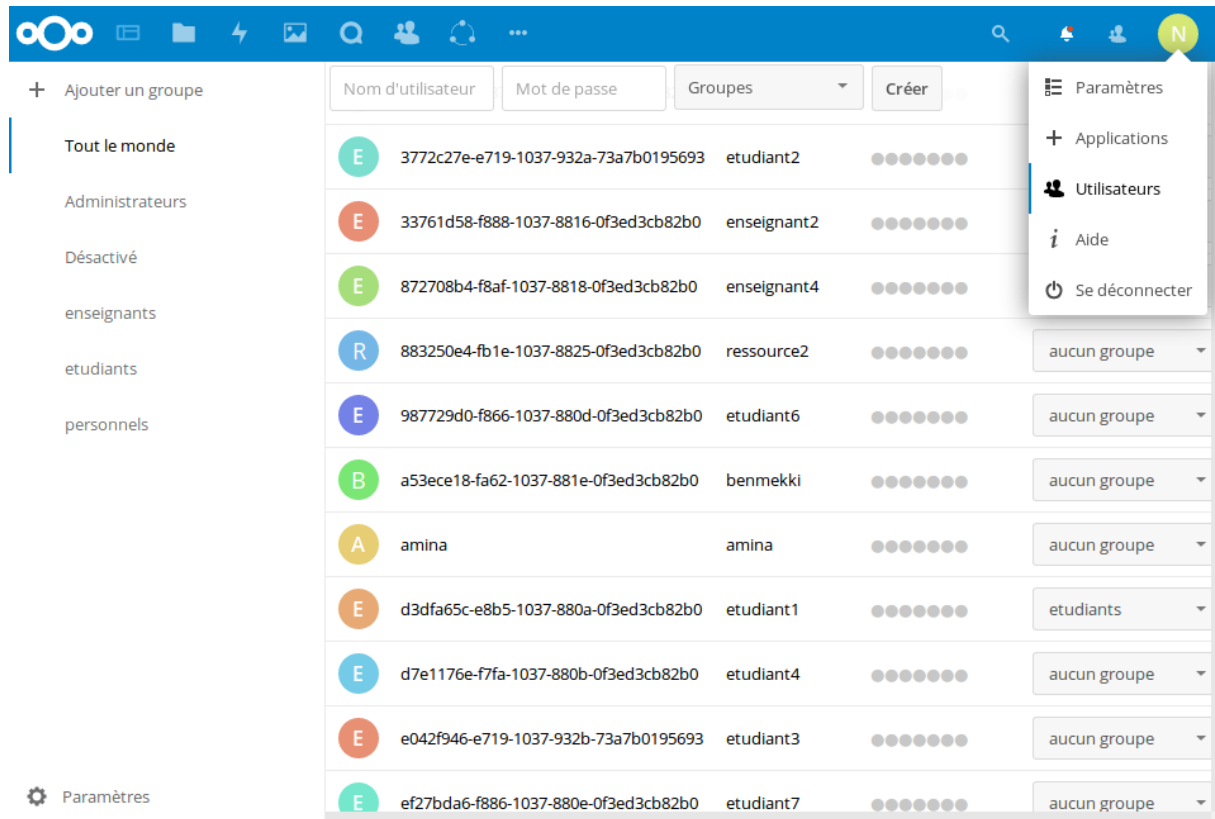


Figure 44 : Gestion des utilisateurs sous nextcloud

3.8.3.2 Gestion des applications existantes dans le nextcloud

Annonces : qui est une application qui permet de faire des annonces simples, contenant un sujet une description et destinataires et peuvent êtres publics dans le cas où on ne précise pas de destinataire. Seuls l'admin de nextcloud et les utilisateurs qui font partie du groupe d'administrateur ont le droit de faire des annonces (public, privé, ou pour un groupe)

Exemple d'une annonce d'un examen dans la figure suivante :

Ajouter une annonce

exam

étudiants M2 ISI
examen à 10h salle 20 |

Groupes...

Ces groupes vont être capable de voir les annonces. Si aucun groupe n'est sélectionné, elles seront visibles par tous les utilisateurs.

Annoncer Options avancés



Figure 45 : Interface de l'api annonce

Annoncer Options avancés

- Créer des activités
- Créer des notifications
- Autoriser les commentaires

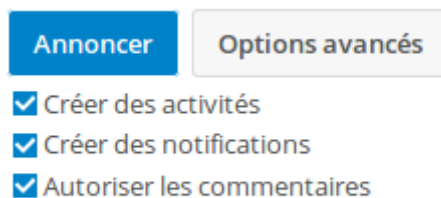


Figure 46 : Restrictions de l'annonce

Aperçu de l'annonce pour un utilisateur

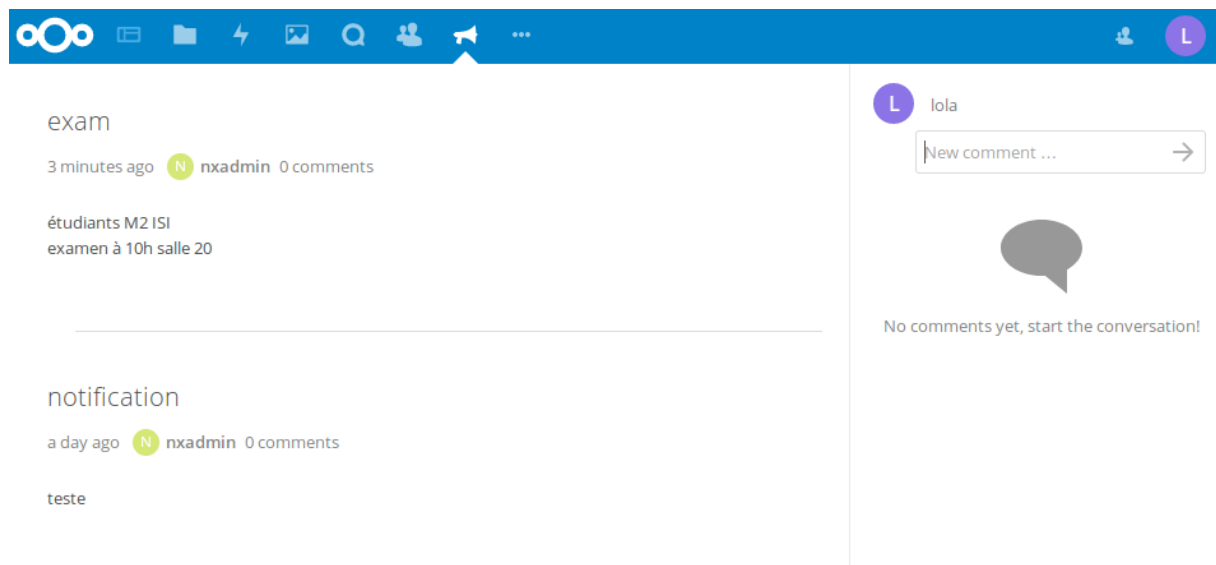


Figure 47 : Interface de l'Annonce

Nextcloud Talk : Nextcloud Talk est un service de communication audio/vidéo et de chat entièrement sur site. Il comprend des applications Web et mobiles et est conçu pour offrir le plus haut degré de sécurité tout en étant facile à utiliser²².

Nextcloud Talk réduit la barrière de communication et permet à votre équipe de se connecter à tout moment, n'importe où, sur n'importe quel appareil, entre eux, avec des clients ou des partenaires.

La figure suivante montre un exemple de discussion :

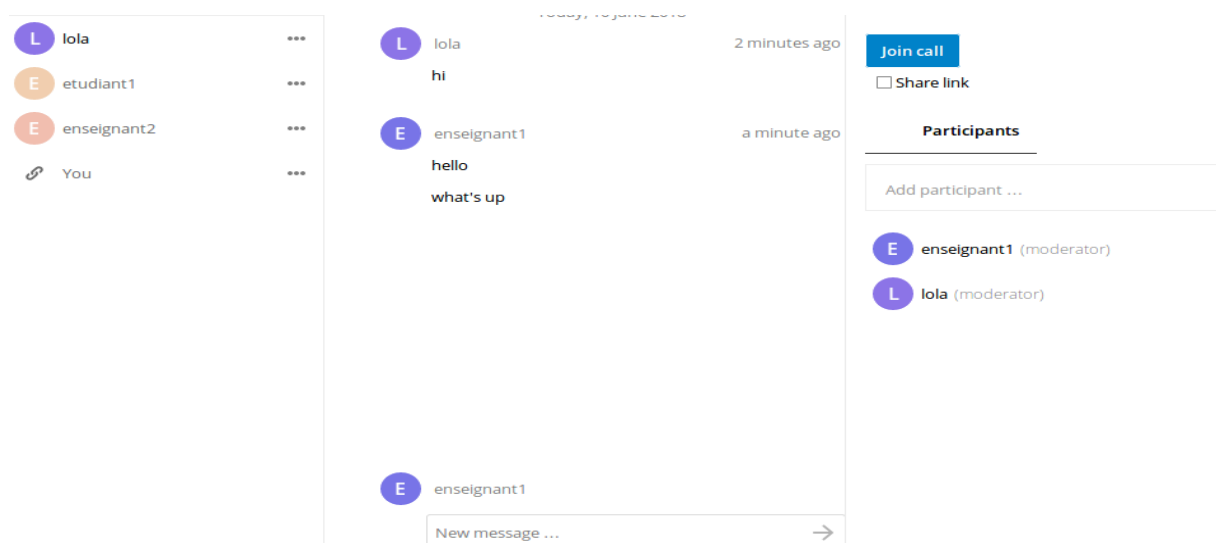


Figure 48 : Interface TALK de nextcloud

CONCLUSION ET PERSPECTIVES

L'objet de ce mémoire était de mettre en place un environnement de travail incluant, un système d'authentification unifiée (SSO) et une messagerie collaborative open source.

Toutefois, ce projet n'est qu'une preuve de concept (POC) d'une architecture qui pourrait répondre aux exigences fournies. Une étude plus approfondie des différentes technologies proposées et leur adaptabilité aux éventuelles évolutions des besoins est nécessaire. Limités par le temps de réalisation et de formation aux multiples technologies rencontrées, nous nous sommes concentrés sur la mise en place d'une architecture minimaliste. Cependant, nous sommes en mesure d'apporter des propositions d'amélioration sur le rendu obtenu à la fin du projet.

Si l'université souhaite mettre en place un système d'information basé uniquement sur des technologies open source. Voici une proposition d'architecture plus complexe et évolutive :

- openldap
- zimbra
- nextcloud
- uportal
- cas/lemonldap

Dans le cas où l'université envisage la mise en place d'un environnement Active Directory afin de proposer des postes avec un système d'exploitation Windows à l'ensemble des actifs, il serait préférable d'utiliser l'annuaire de l'AD afin de gérer les informations d'identification/d'authentification. (Zimbra, AD, Nextcloud / partageSMB, uportal ADFS)

Quelle que soit l'option choisie, plusieurs chantiers complémentaires doivent être entamés avant la mise en place des solutions proposées :

- Définition d'une architecture réseau interne.
- Cloisonnement des différents sous réseau (administration, étudiants, professeurs, ...).
- La mise en place d'une charte d'utilisation du SI.

Bien que l'objectif principal étant l'étude et la mise en place de services pouvant faciliter la gestion administrative et l'interaction enseignants/étudiants, l'aspect sécurité reste toutefois majeur. Il serait judicieux de compléter les résultats obtenus par une analyse de risques et des protections qui doivent être mises en place afin d'assurer les principes fondamentaux de la sécurité notamment la confidentialité, l'intégrité, la traçabilité et la disponibilité.

Références et bibliographies

- [1] ZIMBRA - MESSAGERIE COLLABORATIVE D'ENTREPRISE OPEN SOURCE EPSILON (SAINT-HERBLAIN) SEBASTIEN DEON EDITIONS ENI, 2009
- [2] <http://www.starxpert.fr/zimbra/presentation-de-zimbra/>
- [3] ZCS Administrator's Guide, Open Source Edition, 6.0.8, https://www.zimbra.com/docs/os/6.0.10/administration_guide/2_Overview%20System%20Architecture.03.4.html
- [4] <http://www.starxpert.fr/zimbra/presentation-de-zimbra/>
- [5] <https://zimbra.org/extend/items/view/zimslabim>
- [6] Vincent Mathieu, Pascal Aubry, Julien Marchal, Single Sign-On open-sourceavec CAS http://www.google.cm/url?q=http://www.esup-portail.org/consortium/espace/SSO_1B/cas/jres/cas-jres2003-article.pdf&sa=U&ei=5hPkUba0PPGb1AXlmIGQBg&ved=0CBkQFjAA&usg=AFQjCNH6zxL2y1ShZCCHLYjbYxWRCBzJPw
- [7] <https://www.apereo.org/projects/cas>
- [8] <https://wiki.zimbra.com/wiki/Preauth>, <https://github.com/YPCI/zimbra-cas/blob/master/zimbracas-preauth.jsp>
- [9] <https://www.proxmox.com/en/proxmox-ve>
- [10] <https://www.le-vpn.com/fr/information/>
- [11] <https://openvpn.net/index.php/access-server/overview.html>
- [12] <https://doc.ubuntu-fr.org/ssh>
- [13] <https://www.esup-portail.org/wiki/display/ESUPMU/01+-+les+DLM+uPortal>
- [14] <https://github.com/apache/tomcat>
- [15] <https://doc.ubuntu-fr.org/zimbra> , <https://blog.zimbra.com/2018/01/install-zimbra-collaboration-8-8-ubuntu-16-04-lts/>
- [16] https://wiki.zimbra.com/wiki/Administration_Console_and_CLI_Certificate_Tools
- [17]<https://wiki.jasig.org/DISPLAY/CAS/CASIFYING+ZIMBRA>
- [18]<http://downloads.jasig.org/CAS-CLIENTS/MAVEN-UPLOAD-REQUESTS>

[19] <https://docs.nextcloud.com/server/10/NextcloudDeveloperManual.pdf>

[20] <https://github.com/ZimbraCommunity/owncloudzimlet>

[21] <https://github.com/nextcloud/server>

[22] https://docs.nextcloud.com/server/13/admin_manual/installation/index.html

Autres sites web consultés

<https://www.apereo.org/projects/uportal>

<https://www.apereo.org/projects/uportal/about-portlets>

<https://github.com/YPCI/zimbra-cas/blob/master/zimbracas-preauth.jsp>

<https://wiki.jasig.org/display/UPM40/Building+and+Deploying+uPortal>

<https://www.esup-portail.org/wiki/display/ESUPMU/c%29+Installation>

https://wiki.zimbra.com/wiki/Administration_Console_and_CLI_Certificate_Tools

<https://github.com/Jasig/uPortal-start/blob/master/README.md>

<https://www.esup-portail.org/wiki/display/PROJPORTLZIMBRA/3-+FAQ>