



MIR Messagerie

Auteurs :

Nicolas BROISIN (chef de projet)

Chris CESBRON - Nicolas DOSTERT

Jérôme GOUPIL - Sothirak PHE

Nelson DA SILVA - Benoît CAILLABET

TABLE DES MATIERES

PRESENTATION DU PROJET	3
Introduction	3
Rappel du cahier des charges	4
ETUDE DES PRINCIPALES SOLUTIONS	5
Description des principaux serveurs de messageries collaboratives	5
Synthèse sur les différences de fonctionnalités entre systèmes de messagerie collaborative.....	6
Description des principaux clients de messagerie	7
Synthèse sur les différences de fonctionnalités entre clients de messagerie.....	8
Description des principaux serveurs de messagerie instantanée	9
Synthèse sur les différences de fonctionnalités entre systèmes de messagerie instantanée	10
Description des principaux clients de messagerie instantanée	11
Synthèse sur les différences de fonctionnalités entre clients de messagerie instantanée	11
Bilan de l'étude comparative.....	12
SOLUTION LINUX : LOTUS DOMINO 8.5 ET LOTUS SAMETIME 8.5	13
Introduction	13
Réponse au cahier des charges	13
Etude des fonctionnalités des accès / sécurité de Domino 8.5	13
Etude des fonctionnalités des accès / sécurité de Sametime 8.5	17
Etude des fonctionnalités de messagerie unifiée	19
Etude des fonctionnalités de messagerie collaborative	22
Etude des fonctionnalités de gestion de Lotus Domino 8.5	22
Etude des fonctionnalités de visioconférence et téléphonie.....	24
Etude des fonctionnalités d'administration de Lotus Domino 8.5.....	27
Etude des fonctionnalités d'administration de Lotus Sametime 8.5	28
Déploiement de la solution	29
Architecture logique de Lotus Sametime 8.5.....	29
Architecture physique de Lotus Sametime 8.5	29
Architecture logique de Lotus Domino 8.5	29
Architecture physique de Lotus Domino 8.5	30
Architecture physique globale.....	30
Planning du projet	31
Coût de la solution Lotus Domino 8.5 et Lotus Sametime 8.5	31

SOLUTION WINDOWS : EXCHANGE 2010 ET LYNC 2010	32
Introduction	32
Réponse au cahier des charges :	32
Etude des fonctionnalités des accès de Exchange 10	33
Etude des fonctionnalités de sécurité de Exchange 10.....	38
Etude des fonctionnalités des accès / sécurité de Lync 10	41
Etude des fonctionnalités de gestion d'Exchange 2010	43
Etude des fonctionnalités de messagerie unifiée	45
Etude des fonctionnalités de messagerie collaborative	46
Etude des fonctionnalités de visioconférence et téléphonie.....	47
Etude des fonctionnalités d'administration Lync 2010.....	48
Etude des fonctionnalités d'administration Exchange 2010.....	49
Déploiement de la solution	50
Architecture logique de Lync 10	50
Architecture physique de Lync 10	51
Architecture logique d'Exchange 10	55
Architecture physique d'Exchange 10	57
Architecture physique globale.....	57
Planification du projet	58
Coût de la solution Exchange 10 et Lync 10.....	59
CONLUSION	60
LEXIQUE.....	61
Annexe 1 : Topologie logique de Lotus Domino 8.5	62
Annexe 2 : Topologie physique de Lotus Domino 8.5.....	63
Annexe 3 : Topologie logique de Lotus Sametime 8.5	64
Annexe 4 : Topologie physique de Lotus Sametime 8.5	65
Annexe 5 : Complément de l'architecture téléphonique de Lotus Sametime 8.5	66
Annexe 6 : Planning du projet de Lotus Domino 8.5 et de Lotus Sametime 8.5	67
Annexe 7 : Topologie logique d'Exchange 2010	68
Annexe 8 : Topologie physique d'Exchange 2010.....	69
Annexe 9 : Topologie logique de Lync 2010	71
Annexe 10 : Topologie physique de Lync 2010.....	72
Annexe 11 : Planning du projet d'Exchange 2010 et de Lync 2010	73
Annexe 12 : Besoins matériels d'Exchange et de Lync 2010	74
Annexe 13 : Compléments des Coûts d'Exchange 2010	75
Annexe 14 : Complément des Coûts de Lync 2010.....	76
Annexe 15 : Description des rôles de Lync	77

PRESENTATION DU PROJET

Auteur : Nicolas BROISIN

Introduction

La messagerie électronique est devenue au fil du temps un outil absolument indispensable à toutes les entreprises si elles veulent pouvoir faire preuve de compétitivité et de réactivité. En contrepartie il est vrai que sa gestion et son exploitation sont souvent sources de difficultés. Par ailleurs la messagerie doit être accessible de partout, à tout moment, et offrir des fonctions collaboratives, telles que les agendas et carnets d'adresses partagés ou encore le partage de documents. En matière d'échanges professionnels et de collaboration, les médias sociaux sont encore loin de détrôner l'e-mail.

De plus, la messagerie instantanée devient incontournable car elle vise à améliorer la productivité des collaborateurs et aussi de permettre l'échange plus rapide des informations.

La fusion de la messagerie instantanée avec le courrier électronique et la téléphonie est dorénavant un enjeu primordial, on parle donc aujourd'hui de communication unifiée. Elle consiste à fournir une interface commune à tous ces outils, quels que soient le terminal et le contexte de travail (au bureau, en clientèle, en déplacement).

Afin d'unifier l'ensemble de ces composants, il faut intégrer au système d'information plusieurs solutions :

- un serveur de messagerie collaboratif
- un serveur de messagerie instantanée
- leur client lourd et web léger respectifs.

Après un rappel du cahier des charges, nous allons vous proposer une description synthétique de plusieurs solutions couramment utilisées en entreprise. Après une analyse des résultats, nous vous proposerons de voir plus en détails les deux groupements de solutions retenues. Cela afin de détailler la réponse aux différents besoins de fonctionnalités du client Archimède.

Rappel du cahier des charges

Le client Archimède souhaite mettre en place un système de messagerie collaboratif complété d'une solution de collaboration instantanée. Il souhaite aussi que les solutions choisies prennent en compte la possibilité d'avoir une messagerie unifiée afin de coupler la messagerie et la téléphonie.

Les solutions choisies devront répondre aux fonctionnalités suivantes :

SYNTHESE DU CAHIER DES CHARGES
BESOINS FONCTIONNELLES DU CLIENT
Gestion des agendas, contacts personnels, tâches, demande de réunion
Partage de plannings, mails
Consulter les ressources de l'entreprise : salles de réunion (avec équipements)
Proposition de réunion en fonction des plannings
SECURITE
Possibilité d'envoyer des courriers signé et/ou crypté (S/MIME)
Dispositif des gestions des droits numériques des documents échangés
Stratégie de rétention et d'archivage (gestion du cycle de vie des courriers)
Anti Spam + Scanner Antivirus
Haute disponibilité des données
MESSAGERIE UNIFIEE
Possibilité de recevoir des messages vocaux dans sa boîte aux lettres
Indication de présence
Consultation des mails par téléphone
QUALITES D'INTEGRATION
Faciliter d'intégration de solution dans le SI
Auto configuration du client lourd de Messagerie
Qualité de l'interface web du client online
Interopérabilité avec les OS clients Linux et Windows

ETUDE DES PRINCIPALES SOLUTIONS

Description des principaux serveurs de messageries collaboratives

Auteurs : Jérôme GOUPIL et Nicolas DOSTERT

Fonctionnalités / solutions	Exchange 2010	Exchange 2013	Zimbra	Zarafa	Lotus Domino	Kolab	Citadel
Système de messagerie unifiée	OUI +++	OUI +++	OUI	OUI +	OUI +++	OUI -	OUI -
Gestion de la messagerie	OUI +++	OUI +++	OUI +++	OUI +++	OUI +++	OUI	OUI
Gestion des agendas	OUI +++	OUI +++	OUI +++	OUI +++	OUI +++	OUI	OUI
Contacts	OUI +++	OUI +++	OUI +++	OUI +++	OUI +++	OUI	OUI
Tâches	OUI +++	OUI +++	OUI +++	OUI +++	OUI +++	OUI +++	OUI
Demandes de réunions	OUI +++	OUI +++	OUI +++	OUI +++	OUI +++	OUI	NC
Réservation de divers types de ressources	OUI +++	OUI +++	NC	NC	NC	NC	NC
Synchronisation avec les principales plateformes mobiles (Android, iOS, BB...)	OUI +++	OUI +++	OUI +	OUI +++	OUI	OUI -	OUI
Envoi de courriels signés / cryptés /	OUI+++	OUI+++	OUI	OUI	OUI+++	NON	OUI
Gestion des droits numériques (interdictions ...)	OUI +++	OUI +++	NC	NON	OUI +++	NON	NC
Web Access	OUI ++	OUI +++	OUI ++	OUI ++	OUI	OUI +++	OUI
Simplicité d'administration	NON - (Ligne de commande)	OUI +++	OUI	NON - (Ligne de commande)	OUI ++	OUI ++	OUI +
Accès en lecture / écriture à certaines données de ses collègues	OUI +++	OUI +++	OUI	OUI +++	OUI +++	OUI +++	OUI +
Liaison Active Directory	OUI +++	OUI +++	OUI +	OUI ++	OUI	OUI +	OUI
Protection contre les pourriels	OUI ++	OUI ++	OUI	OUI	OUI	OUI	OUI
Protection contre les virus dans les mails	OUI ++ (Produit Microsoft)	OUI + (Produit non Microsoft)	OUI ++	OUI ++	OUI ++	OUI ++	OUI ++
Gestion des sauvegardes	OUI	OUI +++	OUI	OUI ++	OUI +++	OUI	OUI
Protection des accès externe	OUI	OUI +++	OUI ++	OUI +++	OUI +++	OUI +++	OUI +++
Notoriété	++++	NC	+	-	+++	-	-
Pérennité de la solution	++	++	++	++	++	-	-
Prix de la solution	+	+	-	+	-	+++ Gratuit	+++ Gratuit

(+++ : Très bien, ++ : Bien, + : Correct, - : passable)

Synthèse sur les différences de fonctionnalités entre systèmes de messagerie collaborative

Ce tableau montre bien les différences fonctionnelles des principales solutions du marché des serveurs de messageries. Comme on peut le voir, les solutions Microsoft Exchange 2010 et Exchange 2013 ainsi que Lotus Domino d'IBM sont les trois produits intégrant le mieux une messagerie unifiée.

Zarafa, qui a été développé comme un clone d'Exchange, a des fonctionnalités de messagerie équivalentes aux solutions de Microsoft, mais ne possède pas de connecteur natif pour assurer la liaison à un client de messagerie instantané. Kolab et Citadel ont principalement été développés pour être utilisés par un navigateur web, même si c'est maintenant possible de se connecter à ces messageries via un client lourd, les fonctionnalités de celui-ci étant toutefois limitées. Les certifications électroniques sont devenues un élément extrêmement important dans la sécurisation des échanges numériques. Les solutions Exchange 2010 et Exchange 2013, Lotus Domino et Zarafa intègrent parfaitement ces composants, car ce sont des solutions destinées aux moyennes et grandes entreprises pour lesquelles la sécurité est vitale. Par contre, Kolab et Citadel visent plutôt les petites entreprises et les administrations et n'autorisent pas autant de sécurisation que les grosses solutions Microsoft et IBM. Ces deux solutions ne répondent donc pas pleinement au besoin en termes d'échanges numériques.

Pour ce qui est du socle technique, les solutions de Microsoft et d'IBM sont celles qui proposent les bases les plus solides. En effet, elles sont prêtes à l'emploi, facilement intégrables dans un nouvel environnement, ou un environnement existant, et facilement administrables via des utilitaires graphiques. Sur ce dernier point, on peut notamment comparer à Zarafa dont une partie de l'administration peut se faire en ligne de commande.

La solution Exchange développée par Microsoft est présente ici dans ses versions 2010 et 2013. Celles-ci répondent parfaitement à la demande du client grâce à leurs fonctionnalités. Cependant, leurs fonctionnements se révèlent suffisamment différents pour ne pas considérer la version 2013 comme une simple mise à jour de 2010.

On pourra citer ici par exemple l'optimisation de la topologie grâce à l'inauguration d'une nouvelle architecture de serveur sur Exchange 2013. En effet, certains rôles ont été regroupés sur une seule machine.

De même, Microsoft a souhaité simplifier l'administration d'Exchange, en regroupant l'ensemble des consoles d'administration dans une unique console devenant le centre d'administration Exchange. De plus Exchange 2013 est un produit jeune ce qui fait que le support d'application tierce n'est pas encore existant ou optimal.

D'une manière générale, Exchange 2010 et 2013 sont deux très bons produits s'intégrant parfaitement en entreprise grâce à une large gamme de produits Microsoft annexes, tel qu'Outlook ou Lync. La principale contrainte pour l'adoption d'une solution Exchange est le coût élevé de celle-ci, même si ce prix est justifié par la solidité de la plateforme technique et du support Microsoft.

Description des principaux clients de messagerie

Auteur : Benoit CALLABET

Fonctionnalités / solutions	Microsoft Outlook	Mozilla Thunderbird	Zimbra Desktop	Lotus Note	Evolution
Systèmes d'exploitation compatibles	Microsoft +	Microsoft, Linux +++	Microsoft, Mac, Linux +++	Linux, Mac OS, Red Hat Linux, SUSE Linux, Windows +++	Linux
Serveurs de messagerie compatibles	Exchange	Exchange, autres...	Zimbra	Lotus Domino, Exchange, autres...	Exchange, autres...
Gestion de la messagerie	OUI +++	OUI +++	OUI +++	OUI +++	OUI
Gestion des agendas	OUI ++	OUI via addon Lightning ++	OUI +++	OUI ++	OUI
Contacts	OUI ++	OUI via addon Lightning ++	OUI ++	OUI ++	OUI
Tâches	OUI ++	OUI via addon Lightning ++	OUI ++	OUI ++	OUI
Demandes de réunions	OUI +++	OUI via addon Lightning ++	OUI ++	OUI +++	OUI
Réservation de divers types de ressources	OUI +++	#	#	#	NON
Synchronisation avec les plateformes mobiles (Android, iOS, BB...)	OUI +++	Dépend du serveur	OUI avec configuration serveur +++	OUI +++	Dépend du serveur
Envoi de courriels signés / cryptés signés et cryptés en interne (ou partenaire)	OUI +++	OUI via addon GnuPG et Enigmail +++	Non	OUI +++	OUI
Gestion des droits numériques (interdictions ...)	OUI++	NON	NON	OUI +	NON
Web mail	Outlook Web Access	Dépend du serveur	Zimbra web client	OUI	Dépend du serveur
Simplicité d'administration	Configuration par script et/ou GPO ++	Auto-Configuration ++	Configuration par script +	Monitoring, déploiement et configuration automatisée +++	Configuration par script +
Accès en lecture / écriture aux données des collaborateurs	OUI +++	OUI +	OUI++	OUI +++	NON
Gestion des sauvegardes	Archivage local .pst ++	Archivage local ++	Tout est sur le serveur +++	Archivage local ++	Archivage local ++
Présence en entreprise	Le plus utilisé +++	Très utilisé ++	Rarement utilisé +	Très utilisé +++	Rarement utilisé +
Prix de la solution	Env. 100€ par utilisateur	Gratuit	Gratuit	Env. 50€ par utilisateur	Gratuit

(+++ : Très bien, ++ : bien, + : correct, - : passable, # : information inconnue)

Synthèse sur les différences de fonctionnalités entre clients de messagerie

Le choix du client de messagerie dépend de nombreux paramètres. Le parc informatique du client Archimède étant composé de postes clients Windows et Linux, cette contrainte peut amener à fournir deux clients différents en fonction des systèmes d'exploitation utilisés. De plus ces clients doivent être compatibles avec les serveurs de messagerie de l'entreprise.

Le tableau comparatif ci-dessus nous permet d'exclure Zimbra et Evolution qui ne remplissent pas assez de critères correspondant au cahier des charges.

Le client Microsoft Outlook remplit la totalité des fonctionnalités requis dans le cahier des charges, mais ce client n'est pas compatible avec les postes Linux du parc informatique d'Archimède. C'est pourquoi il devra forcement être complété par un client compatible Linux pour être choisi dans notre solution finale. Outlook reste cependant le client au coût le plus élevé.

Mozilla Thunderbird pourra parfaitement compléter le client Outlook, mais il peut aussi être choisi comme client principal car il est multiplateforme et compatible avec de nombreux serveurs de messagerie. Malgré ses quelques fonctionnalités manquantes, il s'avère être le plus adapté à la composition du parc informatique hétérogène de notre client. Enfin, Thunderbird a pour avantage principal d'être gratuit.

Enfin, Lotus Note peut également être une très bonne alternative à la solution Microsoft. En effet, Lotus est également multiplateforme et possède une grande simplicité d'administration. Il est également moins onéreux qu'Outlook pour un niveau de fonctionnalité équivalent.

Description des principaux serveurs de messagerie instantanée

Auteur : Chris CESBRON et Sothirak PHE

Fonctionnalités / solutions	Lync Server 2010 / 2013	Lotus Sametime Server	Cisco Jabber	Openfire	IntraMessenger	IceWarp
Communication en temps réel	Oui / Oui	Oui	Oui	Oui	Oui	Oui
Communication en différé	Non / Oui	#	#	Oui	Oui	Oui
Indication de présence	Oui / Oui	Oui	Oui	Oui	Oui	Oui
Intégrer à l'annuaire	Oui / Oui	Oui	Oui	Oui	Oui	Oui
Utilisation avec des applications	Oui, avec Office et SharePoint ++	Oui avec Office, SharePoint, lotus notes +++	Oui avec Office, Sharepoint et Lotus Notes +	Non	Non	Oui avec Office, Outlook et Skype +
Accessible en web Access	Oui, avec Lync web app +++	Oui, avec Domino Web Access +++	Oui avec le SDK +	Oui avec SparkWeb ++	Oui par serveur web +	Oui +++
Accessible sur les mobiles	Oui / Prochainement +	Oui +++	Oui ++	Oui avec Spark+ ++	Non	Oui ++
Possibilité d'envoyer des fichiers	Oui / Oui	Oui	Oui	Oui	Oui	Oui
Vidéoconférences *	Oui / Oui	Oui	Oui avec WebEX	Oui	Oui	Oui
* En multipoint et point à point	Oui / Oui	Oui	Oui	Oui	Oui	Oui
* Avec partages	Oui (tableau blanc, bureau, application) +++	Oui (tableau blanc, bureau, application) +++	Oui (bureau) +	Oui (bureau) +	Oui (bureau) +	Oui (bureau, tableau blanc, application) +++
Sécurité	Echange de clés, certificats	Cryptage + authentification	Cryptage avec AES et TLS / SSL	SSL et serveur de certificats	SSL	SSL
Connexion entre serveurs similaires (répartition de charge)	Oui / Oui	Oui	Oui	Oui	#	Oui
Qualité du support	+++	+++	+++	++	++	+++
Plateforme	Windows	Windows / Linux	Windows	Windows / Linux	Windows / Linux	Windows / Linux
Coût	700 €	500 €	#	0 €	0 €	#

(+++ : Très bien, ++ : bien, + : correct, - : passable, # : information inconnue)

Synthèse sur les différences de fonctionnalités entre systèmes de messagerie instantanée

La comparaison ci-dessus sous forme de tableau correspond à l'ensemble des solutions proposées. Certaines ne répondent pas au cahier des charges du client, c'est pourquoi il a fallu faire des choix pour atteindre au mieux les attentes de celui-ci.

En étudiant le tableau, la solution Microsoft Lync apparaît comme l'une des meilleures, car elle comprend toutes les fonctionnalités demandées, excepté la gestion multiplateforme. Parmi Lync 2010 et 2013, les différences ne sont pas flagrantes, étant donné que Lync 2013 propose essentiellement des améliorations des fonctionnalités existantes sur Lync 2010, à part pour l'application mobile, qui n'est pour l'instant pas disponible.

En ce qui concerne Lotus Sametime, qui est très comparable à Lync, on peut considérer que c'est une solution irréprochable, car elle comprend comme Lync, l'ensemble des fonctionnalités demandées, en plus d'être compatible avec les plateformes Windows et Linux, ce qui est un réel avantage face à la concurrence. On peut aussi ajouter que Lotus est un des éditeurs les plus réputés dans les solutions de messagerie, en plus de fonctionner avec le support de qualité d'IBM.

Pour la solution proposée par Cisco, celle-ci souffre du manque d'informations que l'on a pu obtenir sur elle, étant donné que Jabber est plus récent que les deux premières solutions. De plus ses fonctionnalités sont moins développées, étant donné que Cisco ne propose pas de solution de messagerie complète, et n'a donc aucun avantage sur Lync et Sametime, ceci malgré le fait qu'elle s'intègre bien à des clients de messagerie comme Microsoft Outlook, ou encore Lotus Notes. Cette solution ne sera donc pas retenue.

Le serveur Openfire répond dans la globalité aux attentes du client, il est compatible avec tous les systèmes d'exploitation et offre de multiples caractéristiques intéressantes. De plus, ce logiciel est gratuit, sécurisé et accessible sur les Smartphones.

IntraMessenger étant un très bon serveur de messagerie instantanée, il n'offre qu'une solution propriétaire, il ne peut communiquer qu'entre serveur IntraMessenger et qu'entre client de ce type aussi (compatible Windows seulement). Il n'est pas accessible sur une application mobile. Donc ce logiciel ne peut pas totalement répondre à la demande du client.

IceWarp est un serveur vraiment très complet, assez onéreux et dispose de toutes les caractéristiques demandées. En revanche il sera trop onéreux par rapport aux autres solutions retenues.

Description des principaux clients de messagerie instantanée

Auteur : Nelson DA SILVA

Fonctionnalités / solutions	Pidgin	Lotus Sametime	Lync 2010	Lync 2013	Empathy	Ekiga	Gajim
Support Windows	Oui +	Oui ++	Oui ++	Oui ++	-	Oui +	Oui +
Support Linux	Oui +	Oui +	-	-	Oui ++	Oui +	Oui +
Support Smartphone	-	Oui ++	Oui +	Oui +	-	-	-
audio	Linux +	Oui +++	Windows +	Hors linux ++	Linux +	Windows et Linux ++	Linux +
vidéo	Linux +	Hors Linux ++	Windows +	Windows +	Linux +	Windows et Linux ++	Linux +
Partage de fichiers	Oui	Oui	Oui	Oui	Oui		Oui
Déploiement en entreprise	-	Oui ++	Oui +++	Oui +	-	-	-
Partage d'écran	Oui +	Oui ++	Oui ++	Oui ++	Oui +	-	-
Coût	Aucun +	25/112 \$ -	31/107 \$ -	#	Aucun +	Aucun +	Aucun +

(+++ : Très bien, ++ : bien, + : correct, - : passable, # : information inconnue)

Synthèse sur les différences de fonctionnalités entre clients de messagerie instantanée

Les solutions de messagerie instantanée peuvent varier selon plusieurs caractéristiques, tel que la disponibilité, les fonctionnalités et le prix. Ces solutions sont disponibles sur un nombre variable de plateformes, certaines solutions ne sont présentes sur les périphériques mobiles. Leur fonctionnalités est un autre critère permettent de les distinguer, ces fonctionnalités pouvant être variables d'une plateforme à une autre.

Concernant la disponibilité bureautique, les applications sont généralement multiplateforme, seul la solution Empathy n'est pas disponible sur Windows et les solutions Lync sont indisponibles sous linux. Pour les plateformes mobiles aucune solution libre n'est disponible.

Pour les fonctionnalités audio et la vidéo on constate que leurs disponibilités est particulièrement variable d'une solution à l'autre et d'une plateforme à une autre. Concernant la bureautique Ekiga est la solution la plus performante. Par contre concernant l'usage mobile la solution Sametime est la plus aboutie.

Concernant les fonctionnalités de conférence, partage de bureau, bureau blanc. Seules les deux solutions libres sont à exclure. Les solutions propriétaires offre des fonctionnalités avancées tel que le bureau blanc, de partage d'application.

Afin de mieux répondre au cahier des charges nous nous portons vers des solutions propriétaires. La solution Sametime apparait de par ses fonctionnalités et son côté multiplateforme.

Bilan de l'étude comparative

Auteur : Nicolas BROISIN

Afin de clore cette première phase d'étude, suite aux différentes analyses réalisées en amont, nous pouvons remarquer que plusieurs solutions s'avèrent plus pertinentes que les autres.

Il apparaît clairement que la combinaison Exchange et Lync avec leur clients respectifs, dans leur dernière version semblent répondre idéalement aux besoins en terme de fonctionnalités, de sécurité, de messagerie unifiée et de qualités d'intégration. Par ailleurs, son prix et l'interopérabilité inexistante de son client lourd avec les distributions Linux sont un point de réticence pour son adoption. Le client lourd Linux a adopté de préférence du côté de la messagerie électronique serait Thunderbird et Pidgin concernant la messagerie instantanée.

En ce qui concerne Lotus Domino côté serveur de messagerie collaboratif, et Lotus Sametime côté serveur de messagerie instantanée, nous avons là deux solutions complémentaires qui sont au point de vue des caractéristiques techniques aprioris semblables aux leaders sur le marché que sont Exchange et Lync. De plus, son point fort concerne l'interopérabilité sur des systèmes d'exploitation différents, la solution pouvant être installée sur un environnement Linux ou Windows, ainsi que son client lourd, et cela sans pertes de fonctionnalités. Par ailleurs, cette interopérabilité comporte des risques dans la possibilité d'avoir des bugs de compatibilité entre les différentes versions d'OS.

Nous constatons que du côté du monde libre nous avons plusieurs solutions qui sortent du lot. Nous pouvons citer Zarafa pour la messagerie collaborative couplée à Outlook, et OpenFire pour la messagerie instantanée couplée à Pidgin. C'est une combinaison qui pourrait porter ses fruits dans les années à venir, mais ces solutions n'ont pas eu assez de retour en entreprise pour en faire une étude approfondie. L'intérêt de cette combinaison est concrètement son prix d'acquisition, qui est bien moindre comparé aux deux autres groupes de solutions propriétaires.

On peut clairement identifier trois groupes de solutions, un groupe windows, un groupe mixte et un groupe linux qui répondraient aux attentes du client

Nous allons étudier plus en détails seulement deux groupes de solutions :

- Lync 2010 et Exchange 2010 avec en client lourd Outlook 2010 et Lync 2010 côté Windows et Thunderbird et Pidgin côté Linux.
- Et Lotus Domino 8.5 et Lotus Sametime 8.5 avec Lotus Note 8.5 et Lotus Sametime client 8.5.

SOLUTION LINUX : LOTUS DOMINO 8.5 ET LOTUS SAMETIME 8.5

Auteurs : PHE Sothirak, CAILLABET Benoit, CESBRON Chris, DA SILVA Nelson

Introduction

Dans les systèmes des messageries d'entreprise, Lotus une référence incontestable, sérieusement concurrencée par Exchange. Aujourd'hui fournie par IBM, cette solution se divise en plusieurs parties, correspondantes à des fonctionnalités précises de la messagerie.



Réponse au cahier des charges

Durant cette partie, nous étudierons le système de messagerie d'IBM Lotus Domino et Sametime qui répond aux demandes du cahier des charges fourni par Archimède.

Etude des fonctionnalités des accès / sécurité de Domino 8.5

Auteur : CAILLABET Benoit

La solution de messagerie proposée pour notre client Archimède doit remplir les critères essentiels de la sécurité informatique. Premièrement, la messagerie étant un outil connecté et acheminant des données depuis l'extérieur, il est donc nécessaire de contrôler les flux entrants, les menaces venant de fichiers infectés ou malveillants, ainsi que la charge de connexions que pourra supporter le système. De plus, la solution doit être en mesure de fournir un niveau de disponibilité optimal (la messagerie étant un élément clé pour la productivité d'une entreprise), il donc est vital de mettre en place un système de tolérance de pannes et de répartition de charge.

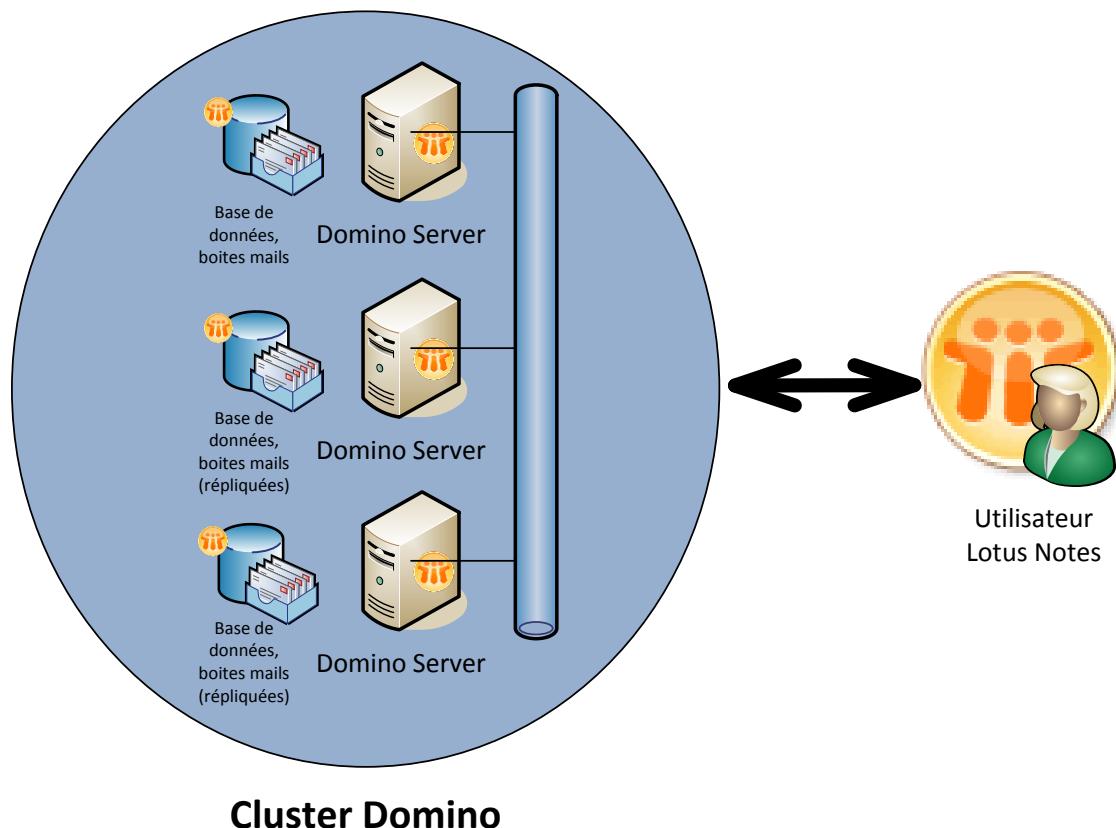
Tolérance de panne / répartition de charge

Afin de répondre aux critères de tolérance de panne et de répartition de charge, Lotus Domino intègre une fonctionnalité de clustering. Cette fonctionnalité est primordiale dans une entreprise de l'envergure d'Archimède.

Le cluster Lotus domino est constitué au minimum de deux serveurs physiques possédant chacun la répliques des bases de données de l'application. Cette réPLICATION permet la continuité du service en cas de panne d'un des deux serveurs, ou encore s'il est nécessaire d'effectuer des opérations de maintenance. Il faut également relever que la réPLICATION entre les serveurs est IMMÉDIATE, il n'y a donc aucune perte de donnée en cas de défaillance de l'un des deux serveurs. Lotus Domino permet de sélectionner les bases que nous souhaitons réPLiquer et leur fréquence de synchronisation.

Cette technologie permet également de partager dynamiquement les ressources des serveurs. Mais surtout, pour répondre à une croissance de l'effectif, il est possible d'ajouter un serveur dans le cluster, et ceci sans interruption de service.

Représentation Logique du Cluster Domino



Reverse- Proxy (serveurs relais)

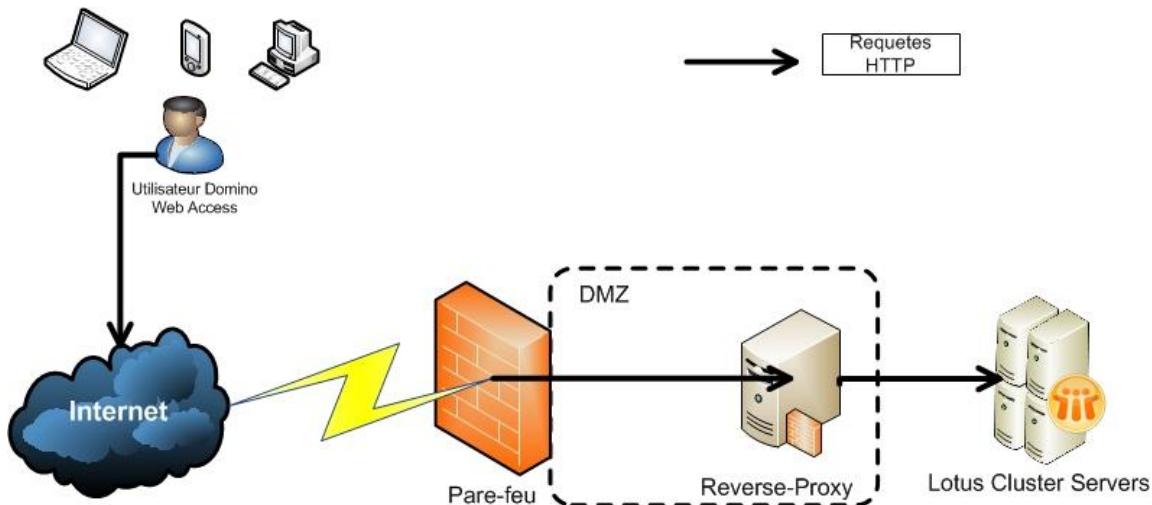
Le cluster Domino intégrera la fonction Domino Web Access. Il s'agit d'un serveur HTTP permettant l'accès aux boîtes mails via un navigateur internet. Bien que le cluster lotus domino offre une première sécurité en cas d'attaques ou de surcharges, il est nécessaire de protéger notre infrastructure à l'aide d'un reverse proxy.

Premièrement, l'infrastructure réseau mise en place (cf. MIR réseau & MIR sécurité) ne permet les accès externes vers les applications de l'entreprise uniquement par le biais d'une DMZ (zone démilitarisée). La DMZ étant une zone du réseau ayant un niveau de sécurité plus faible, il nous est impossible d'y placer nos clusters Lotus Domino sachant qu'ils hébergent les bases de données, et sont donc très sensibles. Les clusters seront donc directement connectés sur le LAN de l'entreprise et protégés par des reverse proxy ou eux-mêmes placé en DMZ.

De plus, cette configuration permettra une mise en cache de certains éléments, ce qui allégera la charge réseau consommée. Enfin, en cas d'attaque informatique provenant d'internet de type DDoS par exemple (Envoi d'un très grand nombre de requêtes dans le but d'un déni de service), le reverse proxy agira comme unurre en devenant la cible de l'attaque à la place de nos clusters Domino.

La solution libre Squid sera employée en tant que Reverse-proxy dans notre infrastructure.

Fonctionnement du Reverse-Proxy



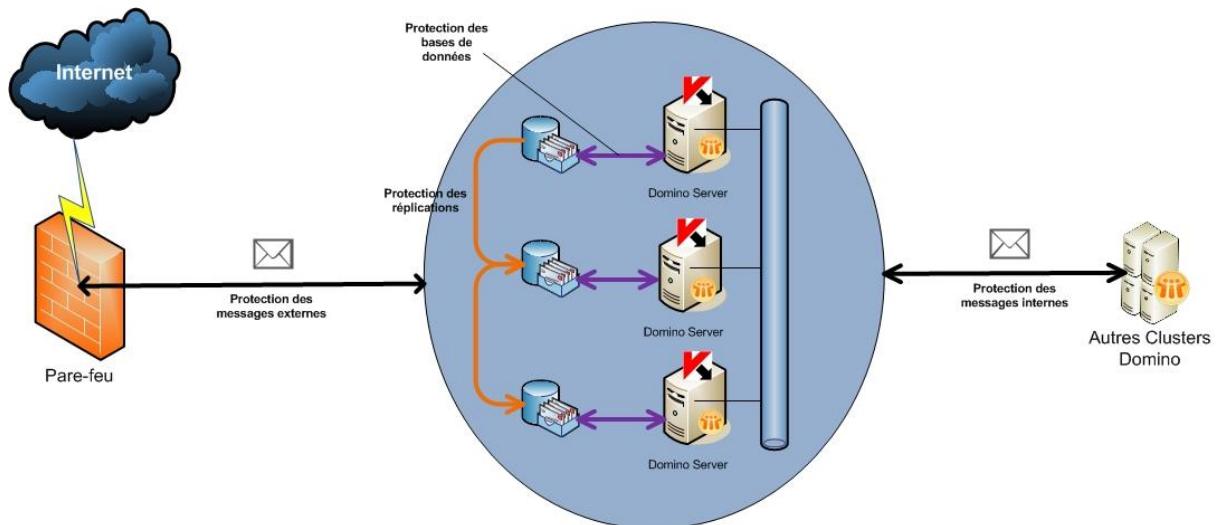
Solution antivirus/ anti malwares /SPAM

Afin de protéger les utilisateurs, et par extension l'infrastructure, des messages indésirables, virus ainsi que des malwares pouvant être introduits via pièces jointes par exemple, la solution Antivirus Kaspersky Antivirus for Lotus Domino s'avère remplir toutes les fonctionnalités requises. De plus, cette version est dédiée pour fonctionner sur un serveur Domino et s'intègre dans le client d'administration. Cet outil sera installé sur les serveurs des clusters Domino, les utilisateurs bénéficieront en plus de la protection locale de leur postes informatiques (Voir MIR Sécurité). L'éditeur Kaspersky est une référence en termes de sécurité sur le marché des solutions de protection informatique.

La solution Kaspersky va offrir les fonctionnalités suivantes :

- Analyse de tous les messages entrants, sortant ou en transit (analyse : texte, pièces jointes, objets OLE)
- Analyse des documents modifiés pendant la réPLICATION
- Analyse des bases de données
- Traitement des objets infectés (avertir et réparer/ supprimer ou ignorer l'objet infecté)
- Notifications des expéditeurs et des destinataires des messages infectés
- Notification sur le risque d'épidémie (empêche la transmission de messages infectés)
- Mise en quarantaine

Logique de fonctionnement de Kaspersky Antivirus for Lotus Domino



Envois de courriers cryptés et/ou signés

Lotus Notes et Domino intègrent les fonctions d'envois de message cryptés et signés, il est possible d'utiliser le standard S/MIME ou le standard Domino.

S/MIME (Secure Multipurpose Mail Extension) permet de garantir la confidentialité et la non-répudiation des messages électroniques. Celui-ci permet la communication sécurisé vers d'autres plateformes compatibles S/MIME telles que Microsoft Outlook. Le standard Domino ne permet des communications qu'entre serveurs Domino. Dans l'idée que certains partenaires d'Archimède auront très probablement le besoin d'envoyer des messages sécurisés sans avoir d'infrastructure Domino, le choix du standard S/MIME s'avère le plus adéquate.

Le standard S/MIME repose sur le principe de chiffrement à clé publique. Les différentes parties d'un message électronique, codées selon le standard MIME, sont chacune chiffrées à l'aide d'une clé de session. Dans chaque en-tête de partie est insérée la clé de session, chiffrée à l'aide de la clé publique du destinataire. Seul le destinataire peut ainsi ouvrir le corps du message, à l'aide de sa clé privée, ce qui assure la confidentialité et l'intégrité du message reçu.

Enfin, concernant la signature des messages, celle-ci est chiffrée avec la clé privée de l'utilisateur. Elle est donc déchiffrable à l'aide de la clé publique mais ceci permet de garantir l'identité de l'expéditeur car seul l'expéditeur est capable de chiffrer un message avec sa clé privée déchiffrable à l'aide de sa clé publique

Etude des fonctionnalités des accès / sécurité de Sametime 8.5

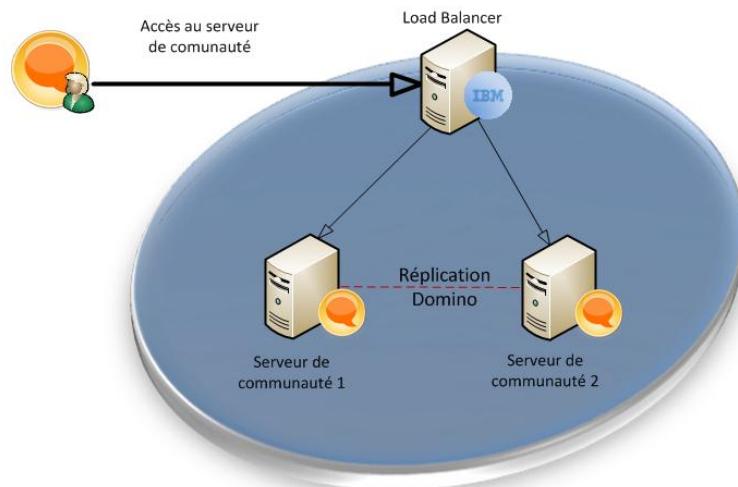
Auteur : DA SILVA Nelson

Haute disponibilité de service

L'échange d'information au sein d'une entreprise étant crucial, il est nécessaire que celui-ci soit fluide et non interrompu. Afin d'assurer la continuité de service, il possible de créer des clusters de serveurs Sametime permettant ainsi la répartition de la charge. Celle-ci peut être assurée par une application telle qu'IBM Load Balancer.

Le rôle Packet Switcher de Media Manager ne peut être intégré dans un cluster. C'est le rôle Conference Manager de Media Manager qui doit assurer la répartition de charge et la continuité de service.

Répartition de charge et continuité de service de serveur de communauté :



Lorsqu'un client veut contacter le serveur de communauté, il contactera l'IBM Load Balancer. Celui-ci redirigera les requêtes en fonction de la disponibilité des serveurs de communauté du cluster.

Afin d'assurer la continuité de service en cas de panne d'un des serveurs du cluster, les informations d'un serveur de communauté sont répliquées sur les autres.

Sécurité de l'information

Au sein d'une entreprise de nombreuses informations sont échangées, dont certaines relevant d'un caractère confidentiel. Il est donc nécessaire de sécuriser leurs échanges, ce que fait Lotus Sametime en implémentant des mécanismes des chiffrements et d'authentification. Virtual Places, le principal protocole de Lotus Sametime, est utilisé pour cela, pendant les phases d'authentification et lors d'échange entre clients par l'intermédiaire d'un serveur mais également pour les échanges entre serveurs. Le mécanisme de chiffrement utilisé est RC2 utilisant une clé 128 bits.

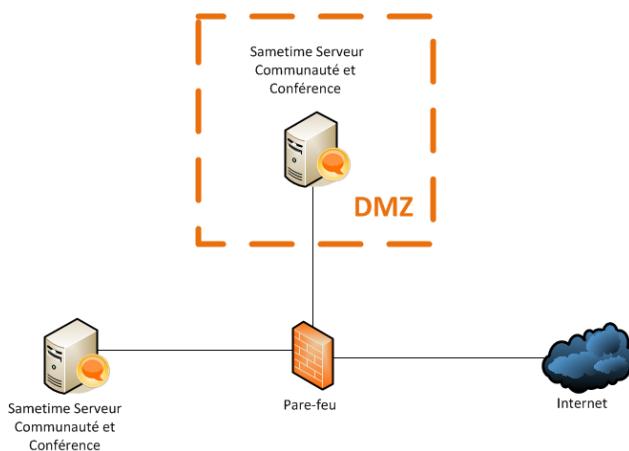
Les conférences reposent sur les normes T.120. Pour y accéder, les utilisateurs sont authentifiés via un Token récupéré au près du serveur de communauté. Il est possible de restreindre l'accès à une conférence à l'aide d'un mot de passe ou par l'utilisation d'une liste blanche.

Concernant la téléphonie unifiée, les clients utilisent les mêmes mécanismes d'authentification. Pour les logiciels de voix sur IP, le protocole de chiffrement TLS est utilisé afin d'assurer la sécurisation de l'authentification SIP. La sécurisation des échanges est quant à elle assuré par le protocole de SRTP.

c. Sécurité des accès externes

Lorsque l'utilisation de Sametime est exclusivement interne, il est aisément de protéger l'infrastructure de l'extérieur en l'isolant de l'Internet. Mais lorsqu'il est nécessaire de communiquer avec l'extérieur alors sa sécurisation se complexifie. Il existe deux cas, pour publier une ressource et pour collaborer avec une autre communauté.

Publication du service de conférence :



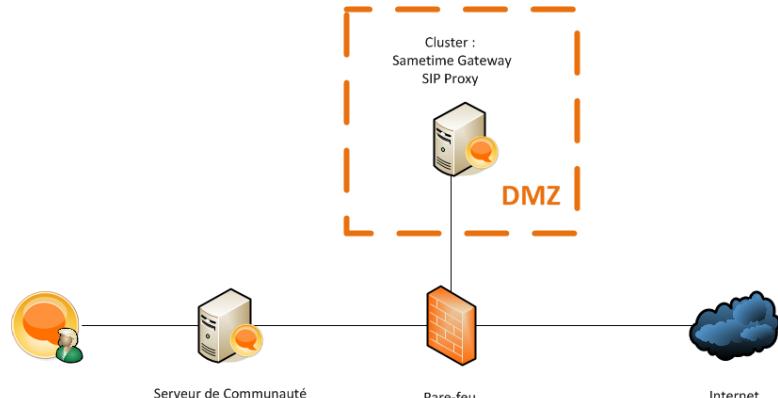
Lorsque l'on souhaite établir une conférence avec un partenaire extérieur il est nécessaire d'exposer une partie de l'infrastructure au monde extérieur. Il conviendra de réduire cette exposition en plaçant la partie à exposé de l'infrastructure sur la DMZ.

Les utilisateurs internes se connecteront au serveur de conférence Sametime interne, les utilisateurs externes, quant à eux, utiliseront le serveur de conférence Sametime situé en DMZ. Ces deux serveurs communiqueront ainsi par l'intermédiaire du firewall. Le serveur sur lequel la conférence a été initiée invitera le second.

Collaborations avec des communautés extérieures :

Afin de collaborer avec une communauté extérieure il est nécessaire de faire appel à un serveur Sametime Gateway. Il conviendra de limiter l'exposition du système d'information en le plaçant en DMZ.

Lorsqu'un utilisateur interne voudra contacter une autre communauté il enverra sa requête au serveur de communauté interne, celui-ci la transmettra au serveur Sametime Gateway situé en DMZ. Ce dernier la retransmettra au serveur gérant la communauté distante. Dans le cas de l'utilisation du protocole SIP, la requête transitera par le proxy SIP.



Etude des fonctionnalités de messagerie unifiée

Auteur : CESBRON Chris



La messagerie unifiée est le regroupement de mails, messages vocaux et de télécopies sur une seule plateforme. Lotus Notes est un outil très utile qui répond à ces critères. La réception de mails émet une notification sonore sur la machine cliente et ce message est écrit en rouge. Chaque personne possède son espace limité en mails, c'est à dire qu'il obtient une quantité limitée de stockage de mail dans sa boîte aux lettres (ex : 250Mo) qui est défini par l'administrateur.

Chris CESBRON - Courier en arrivée - IBM Lotus Notes

Fichier Edition Vue Création Actions Outils ?

Espace de travail Chris CESBRON - Courier en ...

Courrier pour Chris CESBRON

- Courrier en arrivée
- Brouillons
- Envoyés
- Suivi
- Tous documents
- Courrier indésirable
- Corbeille
- Historique des discussions
- Vues
- Dossiers
- Archiver
- Outils

Qui ^	Objet ^	Date ^	Taille ^
nagios	** RECOVERY alert -	27/02/2013 15:43	2K
Support	[Ticket#201302272831] Nouveau ticket	27/02/2013 15:52	2K
Support	[Ticket#201302272832] Nouveau ticket	27/02/2013 15:55	2K
Support	[Ticket#201302272832] Ouverture du ticket : te	27/02/2013 15:55	3K
nagios	** PROBLEM alert - Serveur_ /trap_env_	27/02/2013 16:01	2K
Support	[Ticket#201302272827] Fermeture du ticket	28/02/2013 08:41	3K
NOC	Tr: RE: Perte du lien	28/02/2013 08:58	10K
NOC	Tr: Demande de contact escalade NOC/	28/02/2013 09:03	4K
NOC	Tr: RE: 2019211	28/02/2013 09:05	56K
NOC	Tr: RE: Please arrange Tech + Spare on NOC	28/02/2013 09:11	28K
NOC	Tr: Problème de connexion client	28/02/2013 09:16	12K
NOC	Tr: Intervention POP	28/02/2013 09:17	2K
NOC	Tr: Ticket incident 20086238	28/02/2013 09:20	42K
NOC	Tr: Ouverture ticket d'incident 20121121_	28/02/2013 09:22	13K
Support	[Ticket#201302272825] Fermeture du ticket	28/02/2013 09:33	3K
Support	[Ticket#201302282833] Nouveau ticket	28/02/2013 09:58	2K
Support	[Ticket#201302282834] Nouveau ticket	28/02/2013 10:02	2K
Support	[Ticket#201302282835] Nouveau ticket	28/02/2013 10:21	2K
nagios	Host DOWN alert for	28/02/2013 11:04	2K
Support	[Ticket#201302282836] Demande d'interven...	28/02/2013 11:16	4K
Support	[Ticket#201302282836] Nouveau ticket	28/02/2013 11:16	2K
Support	Re: [Ticket#201302282836] Demande d'interv...	28/02/2013 11:17	4K
Support	[Ticket#201302282836] Fermeture du ticket	28/02/2013 11:17	3K
Support	[Ticket#201302282837] Ouverture du ticket : p...	28/02/2013 11:19	3K
Support	[Ticket#201302282837] Nouveau ticket	28/02/2013 11:19	2K

Prévisualiser ▲

Présent Bureau

Réception de fax sur la plateforme ressemble relativement aux mails :

Chris CESBRON - Courier en arrivée - IBM Lotus Notes

Fichier Edition Vue Création Actions Outils ?

Espace de travail Chris CESBRON - Courier en ...

Courrier pour Chris CESBRON

- Courrier en arrivée
- Brouillons
- Envoyés
- Suivi
- Tous documents
- Courrier indésirable
- Corbeille
- Historique des discussions
- Vues
- Dossiers
- Archiver
- Outils

Date	Type	N°	Etat	Destination	Destinataire	Société
06/10/2005 10:59	FAX	0663	Envoyé	0140096015	cvmfax	
06/10/2005 10:53	FAX	0658	Envoyé	0140096015	cvmfax	
12/12/2003 16:16	FAX	0202	Envoyé	0492966760		
29/05/2008 14:53	FAX	4681	Erreur	0243594360	10TELETECH MAYENN	
29/05/2008 14:50	FAX	4679	Erreur	0243594360	10TELETECH MAYENN	
29/05/2008 14:50	FAX	4680	Envoyé	0188888888	10TELETECH MAYENN	
01/07/2003 09:36	FAX	2960	Envoyé	0143676486	Test	
01/07/2003 09:36	FAX	2960	Envoyé	0143676486	Test	
16/06/2003 16:43	FAX	1394	Envoyé	0143676486	Test	TEST
16/06/2003 16:43	FAX	1394	Envoyé	0143676486	Test	TEST
24/01/2003 16:27	FAX	4649	Envoyé	0143673540	M Jean-Jacques VERVE CVM	
26/07/2006 13:48	FAX	0245	Erreur	0145252636		
14/09/2006 11:35	FAX	2193	Envoyé	0188888888		
10/12/2003 09:48	FAX	5201	Erreur	0143673540	MORNET Marjorie	Communications et VM
29/01/2010 14:37	FAX	1787	Envoyé	0188888888		
29/01/2010 14:37	FAX	1786	Envoyé	0188888888		
29/05/2008 14:52	FAX	4678	Erreur	0565982658		
07/12/2006 14:48	FAX	0913	Envoyé	0144938125	S Lahaye	CommunicationsetVM
07/12/2006 14:29	FAX	0909	Envoyé	0143673540	Dumoleyn	
07/12/2006 14:26	FAX	0908	Envoyé	0143674151	S Verveer	
10/01/2006 12:00	FAX	1732	Envoyé	0143673540	Verveer	CVM
10/01/2006 08:13	FAX	1731	Envoyé	0143673540	Verveer	CVM

Prévisualiser ▲

Présent Bureau

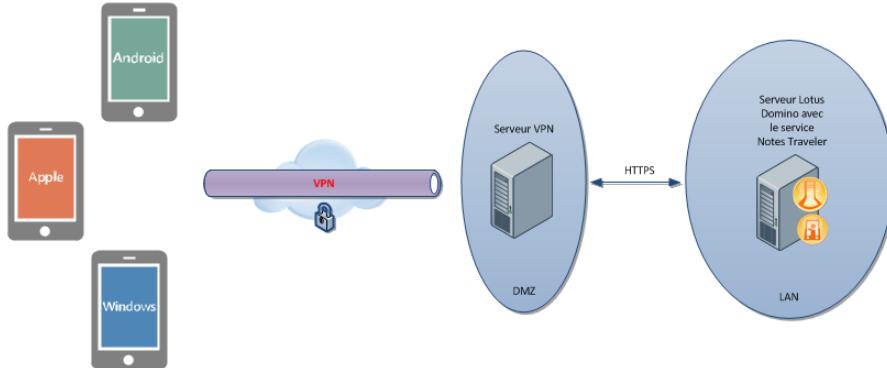
De plus, il est possible d'appeler une personne depuis Lotus Notes, son numéro de téléphone est intégré dans les contacts, ce qui facilite le temps de recherche. L'appel est émis depuis un téléphone fixe, il est possible d'enregistrer la conversation et d'envoyer celle-ci en pièce-jointe ensuite dans un mail.

Consultation de la BAL via le téléphone

Lotus Notes Traveler permet une synchronisation automatique et bidirectionnelle entre les serveurs Lotus Domino et les périphériques de poche sans fil, incluant les périphériques Android, Windows Mobile, Nokia et Apple.

Ce service permet la synchronisation en temps réel des messages électroniques, agendas, listes de tâches, carnets d'adresses et données de journalisation. Les nouveaux courriers électroniques provenant du serveur Lotus Domino arrivent automatiquement sur le mobile et peuvent déclencher un événement de notification.

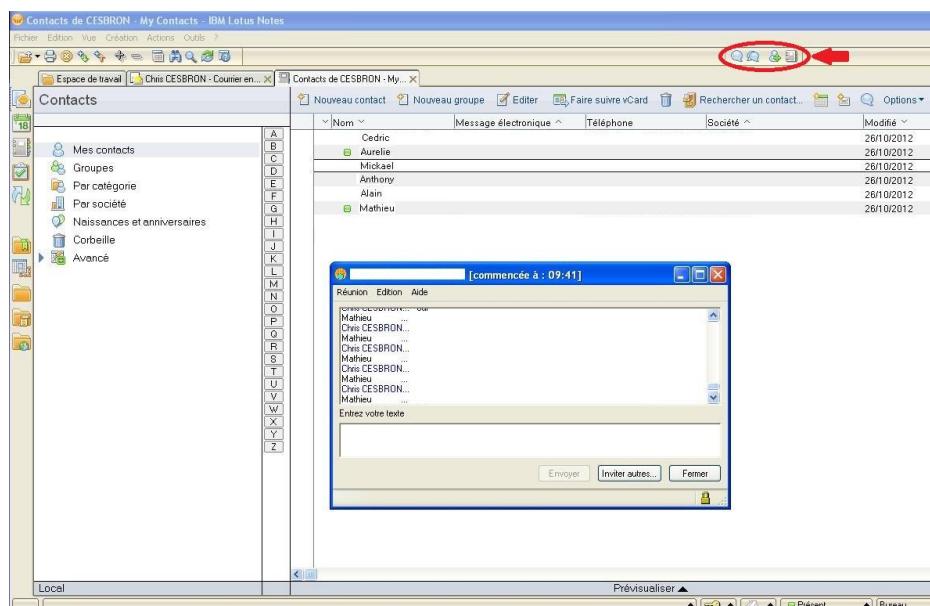
Si vous êtes un utilisateur Lotus Notes ou Lotus iNotes, vous êtes déjà activé comme utilisateur Lotus Notes Traveler. Il suffit aux utilisateurs utilisant leurs ordinateurs de poche d'installer le logiciel client et de pointer sur un serveur Lotus Notes Traveler. Le périphérique est automatiquement enregistré auprès du serveur et sa synchronisation est immédiate.



Le client Lotus Notes Traveler fonctionne avec tous les réseaux privés virtuels (VPN) sécurisés installés sur le périphérique.

La messagerie instantanée Sametime intégrée à Lotus Notes

Il est possible de parler avec un ou plusieurs collègues à partir du client Notes, en utilisant Sametime. Toutes les fonctionnalités de Sametime sont réunies dans un plugin intégré.



Etude des fonctionnalités de messagerie collaborative

Auteur : CESBRON Chris

Lotus Sametime est le logiciel utilisé pour le travail collaboratif. Il est possible d'échanger ces informations entre des salariés internes. Le travail collaboratif étant indispensable pour échanger des données en même temps entre plusieurs salariés et ainsi pouvoir modifier des fichiers avec une multitude de personnes. Avec ce logiciel, il est possible de travailler en collaboration en direct ou bien en différé.

Sametime est intégré dans le logiciel Lotus Notes c'est pourquoi les personnes peuvent avoir leurs mails à proximité. Cela peut donc être utile lors d'un partage de bureau pour reprendre des éléments importants qui ont été reçus.

Sur Sametime, chaque personne peut voir ce qu'un des participants montre sur son écran. Il est possible de modifier les documents par chaque membre de la réunion. De plus, les participants peuvent stocker des fichiers dans un espace collaboratif dédié pour le temps de session de la réunion.

Toutes ces fonctions étant intégrées dans Sametime, il est donc possible de se parler en direct tout en modifiant les documents collaboratifs.

Etude des fonctionnalités de gestion de Lotus Domino 8.5

Auteur : PHE Sothirak

La solution de messagerie Lotus Notes possède de nombreuses fonctionnalités très intéressantes pour les employés d'une entreprise. Nous allons ici vous en présenter quelques-unes, spécifiés dans le cahier des charges.

Gestion des contacts personnels et des tâches

La gestion des contacts est une fonctionnalité importante, car le but d'une messagerie est d'échanger avec ses collaborateurs, et donc il est essentiel que ceux-ci sont accessibles via la messagerie. Pour cela Lotus Notes est assez clair pour les utilisateurs. En effet, lors de la saisie des destinataires, que ce soit pour envoyer un message électronique, ou organiser une réunion, une liste de noms et d'adresses apparaît automatiquement. Ce sont alors les contacts récents qui vont apparaître, ce qui se révèle bien pratique, car lors que l'on échange, on le fait majoritairement avec les mêmes collaborateurs, qu'ils soient dans la même équipe ou autres. Mais si l'un veut contacter un collaborateur qui ne se trouve pas dans les contacts récents, il faudra passer par un annuaire. Celui-ci rassemble l'ensemble des utilisateurs d'un même domaine de serveur de messagerie Domino, ou d'un domaine associé. On pourra ainsi rechercher son contact par des informations (nom, prénom, ID d'entreprise ...).

Lotus Notes propose également une gestion simple des tâches d'un utilisateur. Celles-ci pourront être affectée à des utilisateurs et planifiées dans leur agenda. Ou pourra aussi gérer la priorité de cette tâche, et être classée selon sa catégorie.

Lors de la configuration de la messagerie, on pourra personnaliser toutes ces fonctionnalités, afin de rendre les tâches plus rapides lors d'utilisations fréquentes.

Demande de réunion en fonction des plannings

L'organisation de réunion fait partie intégrante des fonctionnalités de bases de tout système de messagerie, et Lotus Notes n'y fait pas exception. Chaque utilisateur pour créer lui-même une réunion et y inviter des collaborateurs. Mais pour que cette réunion n'entre pas en conflit avec d'autres activités des collaborateurs invités, et ainsi être sûr que chacun pourra assister à la réunion, il paraît essentiel de connaître l'agenda de ceux-ci. Ainsi, si la réunion ne convient pas à un collaborateur, celui-ci aura la possibilité de répondre que l'horaire ne lui convient pas.

Ici aussi toutes sortes de configuration sont possibles selon la nature de la réunion. On pourra ainsi en créer une avec plusieurs collaborateurs, mais sans attendre de confirmation de leur part, pour ne pas surcharger la boîte de réception du créateur de la réunion.

Partage des plannings, mails

Travailler en entreprise, c'est travailler en collaboration avec ses collègues. Pour cela l'agenda est très pratique, car chaque collaborateur pourra voir si son collègue est disponible, que ce soit pour organiser une réunion ou prendre un rendez-vous. Mais chaque personne n'a pas forcément le temps de gérer lui-même son agenda, par exemple un responsable de service surbooké. Dans ce cas-là, ce dernier devra passer par l'étape de délégation, pour donner à un autre utilisateur, une secrétaire de direction par exemple, le droit d'éditer son agenda. Cette dernière personne aura donc, en plus de son agenda personnel, l'accès à l'agenda de son collègue.

Cette délégation peut se faire aussi pour les contacts le courrier et les tâches. Ainsi un utilisateur pourra donner les droits en édition des fonctionnalités les plus pratiques de notes à un collaborateur.

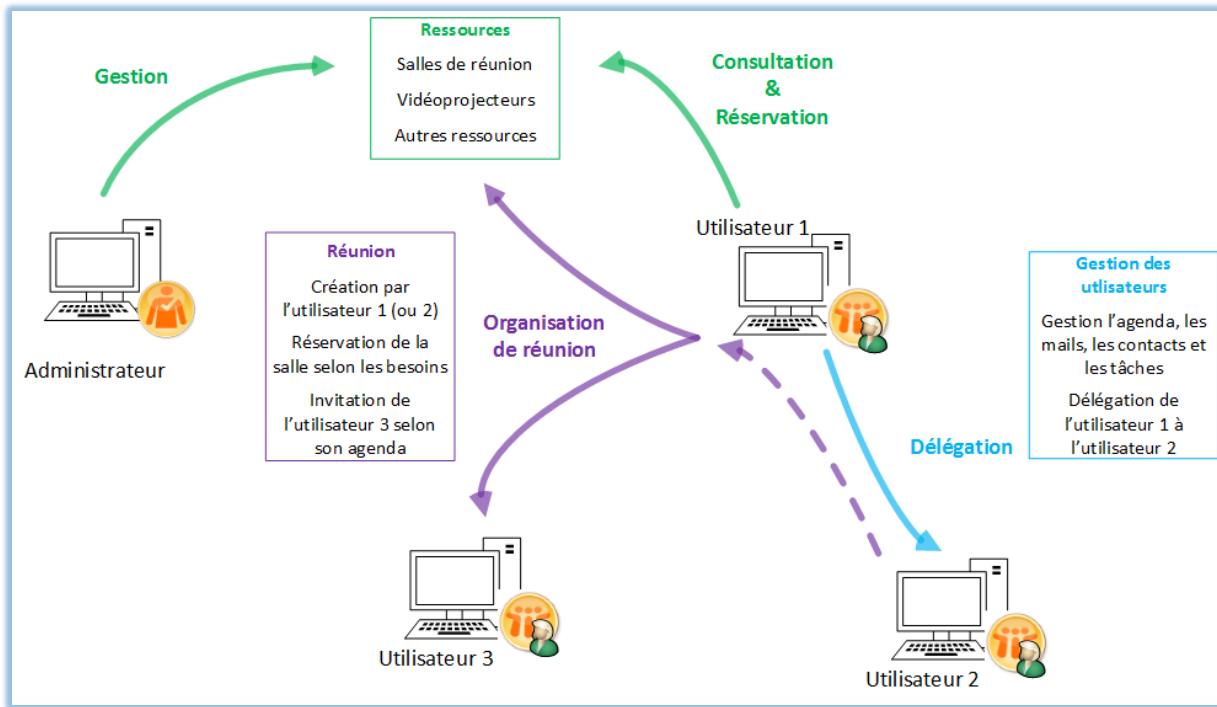
Consultation des ressources

Lors de la création d'une réunion, le rassemblement de toutes les collaborateurs invité est certes essentiel, mais la réservation de ressources qui vont permettre le bon déroulement de la réunion, tel que la salle, les équipements audio visuels ou informatiques ...

Lotus Notes propose la réservation de ces ressources, par le biais de l'option « Trouver des salles » ou « Trouver des ressources ». On pourra ainsi consulter un carnet d'adresses la localisation de la salle ou de la ressource. Pour aider l'utilisateur dans son choix, les informations sur les ressources sont essentielles, comme le nombre de places dans une salle, ou la disposition d'un vidéoprojecteur. Le rôle de l'administrateur sera de mettre à disposition ces ressources sur le serveur Domino. Il pourra aussi spécifier des droits particuliers sur certaines ressources, pour par exemple empêcher la réservation d'une salle mise à disposition pour la direction uniquement. Dans ce dernier cas, seules les secrétaires de directions auront le droit d'édition.

Schéma représentatif

Pour représenter les fonctionnalités décrites ci-dessus, nous allons les appliquer dans des contextes, et expliquer le fonctionnement Lotus Notes avec Domino. Donc ici nous avons un utilisateur 1 qui souhaite déléguer ses tâches de gestion à l'utilisateur 2, et ceci grâce à la délégation. Ce dernier va alors pouvoir créer une réunion pour le compte de l'utilisateur 1. Il va pouvoir inviter l'utilisateur 3 s'il est disponible, et réserver une salle de réunion dans les ressources. Celles-ci sont mises à disposition et gérées par l'administrateur sur sa console.



Etude des fonctionnalités de visioconférence et téléphonie

Auteur : CESBRON Chris

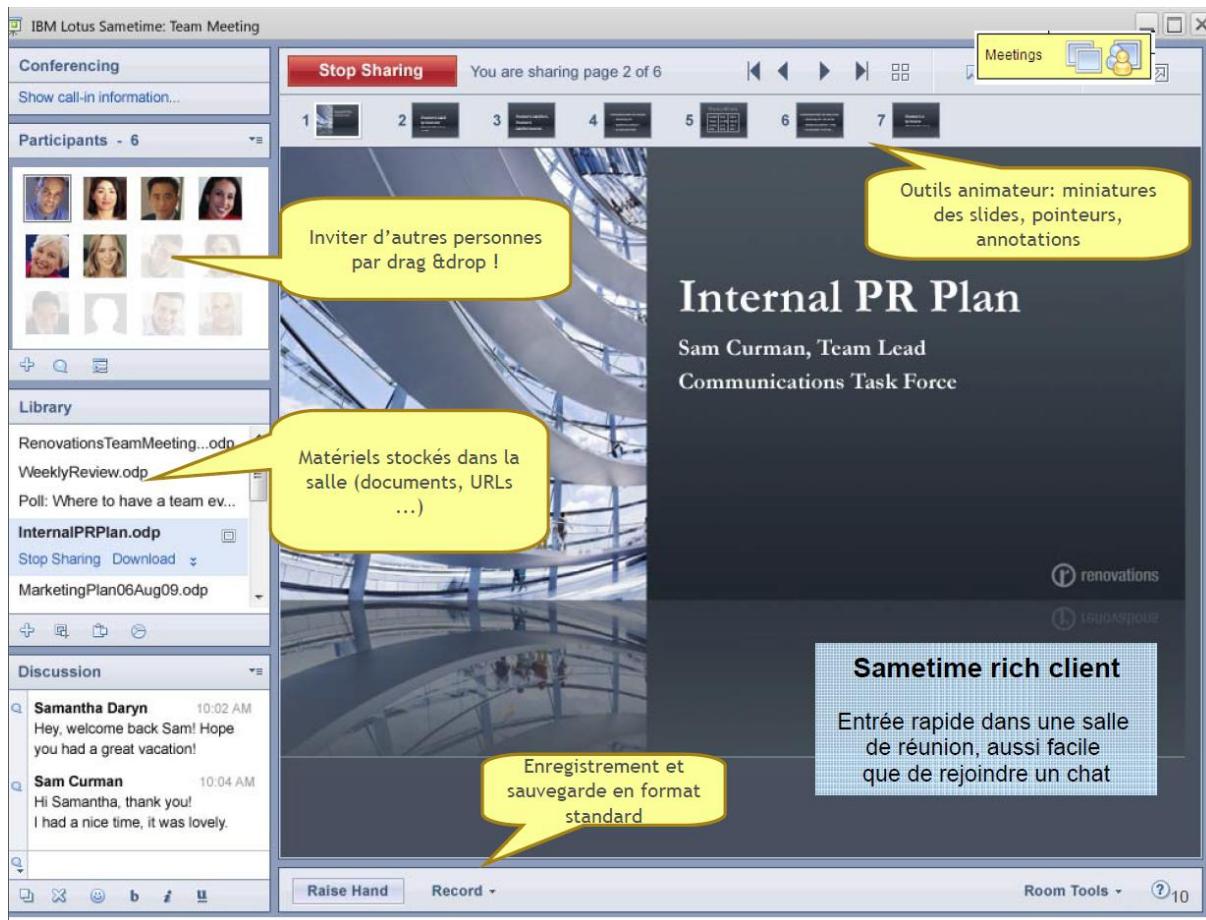


Lotus Sametime propose les technologies de visioconférence et de téléphonie. Ce logiciel peut être accessible depuis un client lourd ou tout aussi bien depuis un navigateur web. Il possède différents composants sur le serveur, étant des rôles à installer. L'ensemble créé la solution Sametime.

Etude de la visioconférence

La visioconférence est une technologie qui inclue la visiophonie et le fait d'être multipoint, c'est à dire qu'il est possible de se connecter à plusieurs sur un même outil pour se voir et se parler mutuellement. Très utilisé en entreprise pour réaliser des regroupements de personnes pour échanger des informations souvent importantes.

Interface utilisateur



Cette interface logicielle offre une facilité d'utilisation, l'ensemble des outils principaux sont rassemblés sur cette interface, qu'elle soit client lourd ou client web.

Un utilisateur peut créer une réunion et inviter des participants qui s'afficheront avec leurs photos, il est possible de lancer une discussion personnelle avec un seul destinataire ou bien groupée en créant une sorte de sondage ou message de diffusion où tout le monde peut répondre. Chacun des participants peut déposer des fichiers dans une bibliothèque temporaire réservée pour la réunion dans le but de partager ces données à l'ensemble du groupe. La gestion de ces fichiers est simplifiée en faisant du « drag and drop » qui signifie « glisser et déposer », c'est un gain de temps.

La qualité du son et de la vidéo ont été très améliorée dans la dernière version Sametime 8.5, mais la latence du réseau affecte la qualité c'est pourquoi il faut tout de même un bon débit de connexion entre les clients et le serveur, puis entre le serveur du client Archimède et Internet.

Il est possible de partager un écran, l'interlocuteur principal peut montrer son écran à tous les autres pour faire une présentation d'un diaporama par exemple. Lorsqu'un groupe travaille sur un document commun et veulent le modifier en collaboratif ils peuvent prendre le contrôle à plusieurs sur ce document affiché à partir d'un écran d'un des participants. Il est également possible d'enregistrer et de sauvegarder les vidéos conférences dans le cas où il s'agirait par exemple d'une présentation importante que l'on souhaite conserver.

En plus de la voix par microphone, il est possible d'écrire des messages dans une boîte de dialogue située sur cette interface. Un des participants ne possède pas de micro, alors il peut tout de même écrire à ses collaborateurs dans cette réunion.

Sametime Media Manager

C'est un des composants de Sametime, il est indispensable car il est utilisé pour acheminer les messages SIP vers une destination. Il se charge d'envoyer et de recevoir les flux média, il travaille sur ces flux pour déterminer le flux global audio/vidéo à servir aux participants. La gestion des réunions est mise en place par ce composant, c'est lui qui détermine le type de réunion, point à point dans la cadre d'une conversation entre deux personnes seulement, multipoint à partir de trois personnes.

Media Manager s'appuie sur SIP pour supporter la VoIP. Il peut être connecté à des systèmes d'Audio et de Visio-conférence pour les intégrer aux conférences et fournit ensuite une interopérabilité entre les clients Sametime et ces points terminaux Audio-Vidéo. Media Manager n'est pas un PBX à part entière. C'est seulement un point de connectivité pour adapter les autres systèmes. Les composants du Media Manager peuvent être dispatchés sur plusieurs machines et aussi le Media Manager peut être clusterisé pour la sécurité et la répartition de charge.

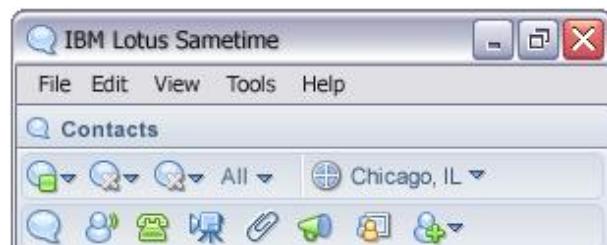
Etude de la téléphonie

Media Gateway



Cet équipement permet de transformer le flux analogique en flux compatible sur le réseau IP. Dans notre cas, des contacts extérieurs peuvent essayer de joindre un correspondant depuis un téléphone analogique vers un téléphone IP interne. La discussion vocale est l'une des deux fonctions de téléphonie du client Sametime qui est utilisée avec le téléphone IP. L'autre est l'appel en un clic qui permet à un utilisateur de créer instantanément une conférence téléphonique avec un ou plusieurs autres utilisateurs.

Dans les deux cas, un utilisateur invite d'autres utilisateurs dans une fenêtre de discussion ou la liste de contacts à se joindre à un appel, et les invités peuvent accepter ou non l'invitation. Toutes les personnes connectées communiquent avec leurs ordinateurs.



➔ Voir un complément de l'architecture téléphonique préconisée pour le client Archimède en annexe 5 (page 66)

Etude des fonctionnalités d'administration de Lotus Domino 8.5

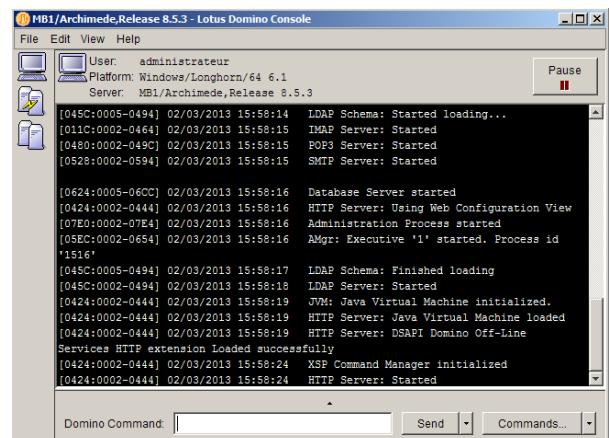
Auteur : PHE Sothirak

L'importance de la messagerie en entreprise fait que son administration un rôle critique. Dans une architecture Domino, on peut distinguer deux moyens d'administrations :

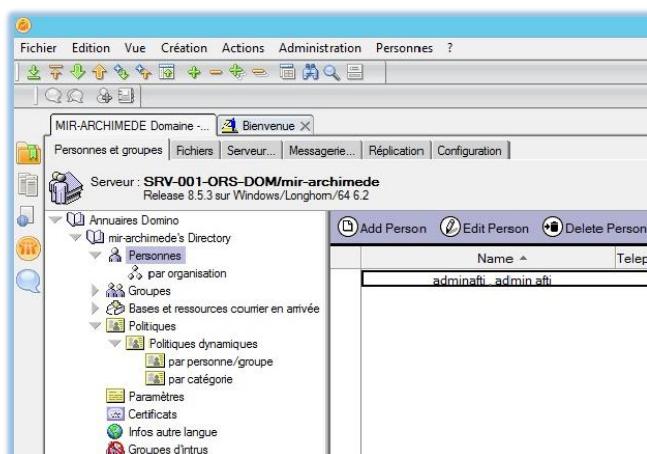
a. Administration avec la console

Ce type d'administration est celle fournie de base avec le serveur Domino. C'est en fait une console d'administration dans laquelle on se connectera à n'importe quel serveur Domino. Mais cette méthode possède un inconvénient, car tout se fait en ligne de commandes. L'administrateur de la messagerie devra donc obligatoirement connaître toutes les commandes nécessaires à l'administration. L'administration en ligne de commande servira donc surtout lors de l'installation de notre premier serveur, afin de créer notre domaine de messagerie.

Ci-dessous, une capture d'écran de la console de Domino.



b. Administration avec le client



Lotus Notes, le client de messagerie de notre solution est fourni avec plusieurs autres composants, dont le client d'administration Domino Administrator. On ajoutera donc cette fonctionnalité au client Notes de l'administrateur de la messagerie du client Archimède. Cette console d'administration possède en plus l'avantage d'être en mode graphique, et donc de simplifier l'administration au quotidien, comme pour ajouter de nouvelles ressources, de nouveaux comptes, ou gérer la sécurité.

Ci-dessous, une capture d'écran du client Lotus Domino Administrator.

Etude des fonctionnalités d'administration de Lotus Sametime 8.5

Auteur : CESBRON Chris

Les outils d'administration de Sametime sont accessibles depuis un navigateur web. Ils sont regroupés en six groupes de fonctionnalités. :

Server Overview : Permet d'obtenir la liste des services ainsi leur état. L'affichage n'est pas en temps réel, il est nécessaire de rafraîchir l'affichage pour obtenir les dernières informations. Il n'est pas possible de démarrer ou arrêter un service, pour cela il faut utiliser les outils d'administration pour Windows.

Message From Administrator : Permet à l'administrateur d'envoyer un message à l'ensemble des utilisateurs connectés. Cette fonctionnalité permet, par exemple, de prévenir les utilisateurs d'une maintenance programmée des serveurs.

Monitoring : Contient plusieurs outils permettant d'obtenir des statistiques en temps réel sur les serveurs, de savoir quel sont les outils utilisés en conférence et par quel utilisateurs ainsi que de connaître l'utilisation des services à un moment donné. Il est ainsi possible d'obtenir les statistiques sur le nombre d'utilisateur authentifiés, connaître le nom des conférences en cours et le nombre de participants.

Logging : La Journalisation, permet d'enregistrer les statistique et autre évènements de Sametime, tel que : Les connexion/déconnexion au serveur de communauté, les échecs d'authentification, les connexions aux serveurs, les statistique des conférences et les alerte de capacités. Il est possible d'afficher les journaux provenant de Domino.

Directory : Cet outil est utilisé pour la gestion des utilisateurs et des annuaires. Il permet la création/suppression des utilisateurs, le changement de mot de passe, la modification des informations d'un utilisateur, la manipulation des groupes.

Configuration : Ce groupe permet la configuration des serveurs Sametime et leur connectivité à travers quatre fonctionnalités :

- Connectivity : Permet la modification des paramètres de connexion entre les serveurs et avec les clients.
- Community Services : Permet de paramétrier les services de communauté et de gérer les droits des clients.
- Meeting Services : Permet de configurer les services de conférences et de gérer la sécurité des clients.
- Audio/Video : Permet de configurer tout paramètre relatif aux flux audio ou vidéo.
- Business Card setup : Permet de choisir quel information seront visible dans la fenêtre de messagerie instantanée.

Déploiement de la solution

Architecture logique de Lotus Sametime 8.5

Auteur : CESBRON Chris

Lotus Sametime est composé de nombreux rôles. Les clients se connectent aux différents serveurs selon les services désirés. Le serveur de communauté est contacté pour l'authentification, pour la messagerie instantanée et l'indication de présence. Le proxy est utilisé par le client web. Les serveurs de Media Manager sont contactés pour les échanges de flux audio et vidéo. Le serveur de base de donné, qui n'est pas un serveur Sametime n'est jamais contacté par les clients, il est utilisé par des serveurs tel que le serveur de conférence. Le serveur Gateway est contacté par l'intermédiaire du serveur de communauté.

→ **Voir la topologie logique de Sametime en annexe 3 (page 64)**

Architecture physique de Lotus Sametime 8.5

Auteur : CESBRON Chris

Lotus Sametime est composé de nombreux rôles. Les clients se connectent aux différents serveurs selon les services désirés. Le serveur de communauté est contacté pour l'authentification, pour la messagerie instantanée et l'indication de présence. Le proxy est utilisé par le client web. Les serveurs de Media Manager sont contactés pour les échanges de flux audio et vidéo. Le serveur de base de donné, qui n'est pas un serveur Sametime n'est jamais contacté par les clients, il est utilisé par des serveurs tel que le serveur de conférence. Le serveur Gateway est contacté par l'intermédiaire du serveur de communauté.

→ **Voir la topologie physique de Sametime en annexe 4 (page 65)**

Cette topologie est identique sur les sites d'Orsay et de Bruxelles, c'est la future architecture physique pour la messagerie Sametime. Les différents rôles sont répartis sur les ESX, l'ensemble des serveurs seront virtualisés sous Centos. Les clients possèderont Lotus Notes et Sametime d'installés.

Il y aura quatre ESX qui seront sur le LAN dans lequel l'ensemble des rôles sera réparti sur différentes machines virtuelles. Les serveurs physiques sont donc redondés en cas de panne.

Virtual Places (VP) : protocole propriétaire utilisé dans Sametime pour les communications entre les clients et les applications serveur et le serveur Sametime.

Architecture logique de Lotus Domino 8.5

Auteur : CAILLAbET Benoit

Voici le schéma logique récapitulant l'infrastructure Lotus Domino proposée.

→ **Voir la topologie logique de Domino en annexe 1 (page 62)**

Architecture physique de Lotus Domino 8.5

Auteur : PHE Sothirak

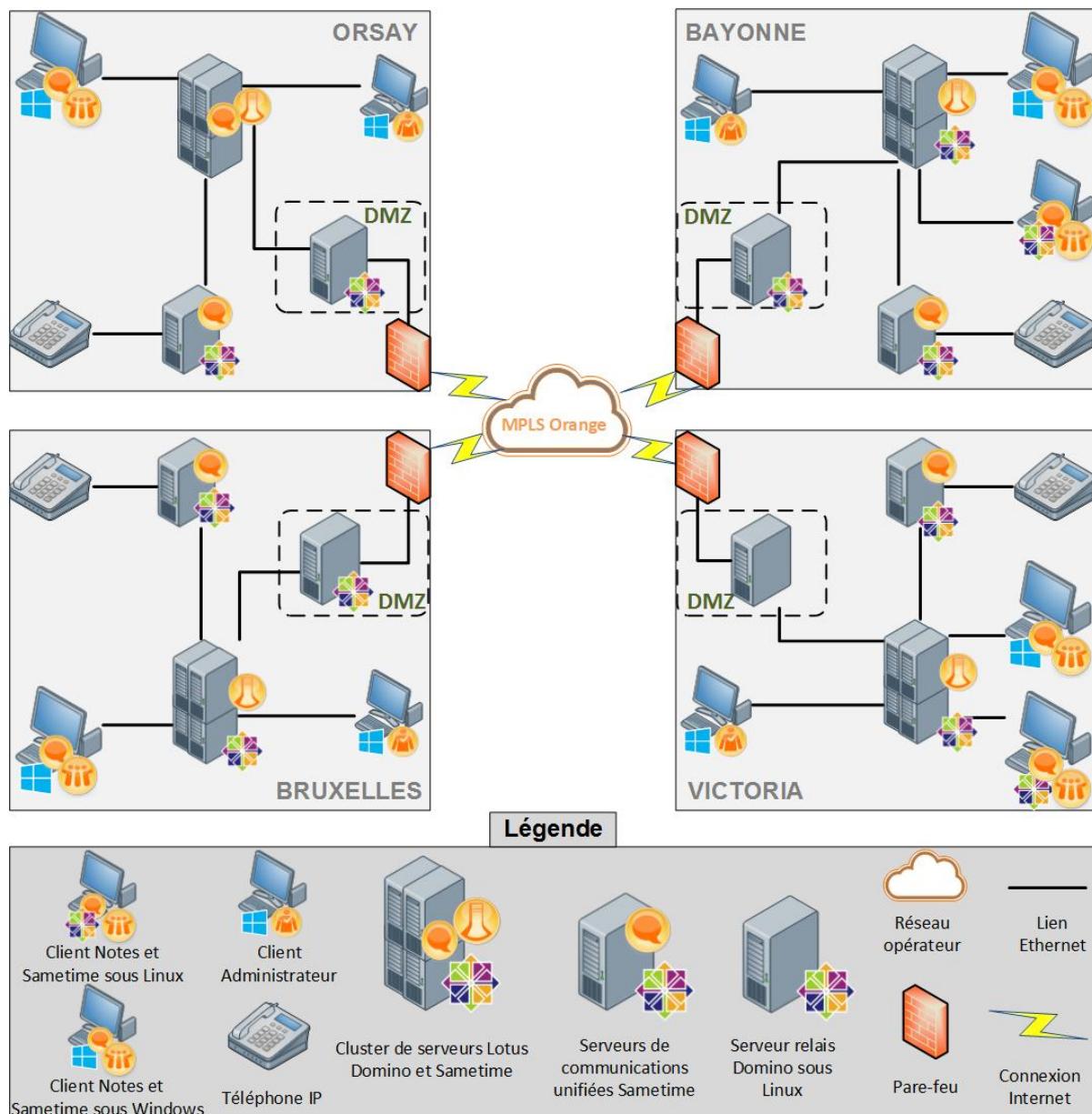
L'architecture suivante décrit comment se composera la future architecture de la messagerie Domino. Celle-ci va s'orienter autour des serveurs Domino qui contiendront les rôles de messageries, vues dans la partie topologie de domino. Chaque site contiendra un serveur Domino sous Windows, et un autre sous Linux avec le rôle Sametime installé. Les clients Linux et Windows quant à eux seront installé sur tous les postes.

→ Voir la topologie physique de la solution Domino en annexe 2 (page 63)

Architecture physique globale

Auteur : PHE Sothirak

L'architecture de Lotus Domino et Lotus Sametime pour le client Archimède a été présenté. L'architecture suivante ressemble les deux solutions et montrent comment ils s'intègrent ensemble pour les quatre sites.



Planning du projet

Auteur : PHE Sothirak

Le planning présenté vous présente les différentes étapes du planning, ainsi que leurs durées. On peut alors mieux comprendre comment se déroulement la mise en place du système de messagerie Lotus Domino avec Sametime. La durée totale pour la mise en place des solutions Lotus Domino et Sametime sera donc de **90 jours** selon nos prévisions.

➔ Voir annexe le planning du projet en annexe 6 (page 67)

Coût de la solution Lotus Domino 8.5 et Lotus Sametime 8.5

Auteur : CAILLABET Benoit

Voici le tableau récapitulant le cout de l'ensemble des besoins nécessaires à la bonne conduite du projet

Description	Coût
12 licences Lotus Domino /Sametime	Inclus licence utilisateur
12 licences Kaspersky Anti-virus for Lotus Domino	16 000 €
4 serveurs Dell Poweredge (Reverse-proxy)	10 000 €
12 serveurs Dell Poweredge (Serveurs Domino)	44 400 €
10 serveurs Dell Poweredge	37 000 €
10 Licences Vmware	50 000 €
Licence Lotus Note 1000 clients	150 000 €
Licence Lotus Sametime 1000 clients	90 000 €
Total	397 400€

SOLUTION WINDOWS : EXCHANGE 2010 ET LYNC 2010

Auteurs : BROISIN Nicolas, GOUPIL Jérôme, DOSTERT Nicolas

Introduction



Microsoft Exchange server 2010 est un système de messagerie collaboratif d'entreprise développé par Microsoft. Microsoft Exchange Server 2010 est la version la plus mature de la solution exchange de Microsoft.



Microsoft Lync Server 2010, évolution de la plateforme OCS 2007 R2, offre une solution de communications optimisée qui vous permet de trouver et de communiquer avec la personne appropriée, en temps réel, à partir des applications que vous utilisez le plus, telles que le client de messagerie Lync et celui de collaboration Microsoft Outlook.

Réponse au cahier des charges :

Réponse du cahier des charges :

Nous avons perçu plusieurs enjeux majeurs lors de la lecture du cahier des charges concordant avec le souhait de fournir aux collaborateurs de la compagnie Archimède un outil de communication efficace :

- Mise en place d'une solution de messagerie instantanée
- Mise en place d'une solution de Web Conferencing
- Appréhender les nouvelles fonctionnalités de téléphonie

Etude des fonctionnalités des accès de Exchange 10

Auteur : Nicolas DOSTERT

Lors de l'installation d'un client de messagerie il est nécessaire de configurer les informations du serveur de messagerie et les informations d'identification du compte de l'utilisateur.

Dans un environnement Exchange il est possible de faire cela de manière classique, c'est-à-dire de passer sur chaque poste pour le faire manuellement, ou de manière automatique, sans intervention de la part de l'administrateur.

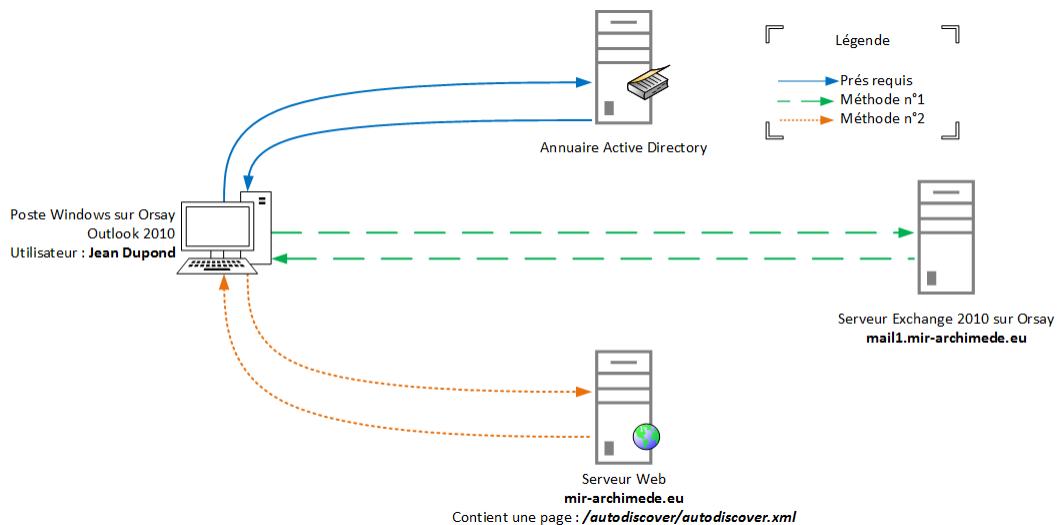
Pour rappel, sous l'environnement Windows notre client de messagerie sera Outlook 2010 et sous l'environnement Linux notre client de messagerie sera Mozilla Thunderbird 17.

Auto configuration Outlook 2010

Microsoft fournit cinq méthodes pour permettre l'auto configuration d'un client Outlook 2010. Préalablement à une tentative d'auto configuration le client doit réaliser deux actions : récupérer l'adresse électronique de l'utilisateur en se basant sur le service Active Directory et récupérer le nom du serveur Exchange de la même façon.

Une fois ces prés requis remplis l'auto configuration commence :

- ✚ Demande direct de la configuration au serveur de messagerie.
- ✚ La découverte automatique d'un fichier de configuration XML grâce au nom de domaine.
- ✚ Utilisation d'un fichier de configuration XML présent sur le poste de travail.
- ✚ Auto configuration en utilisant uniquement le nom du serveur Exchange.
- ✚ Utilisation des paramètres de découverte « standard»



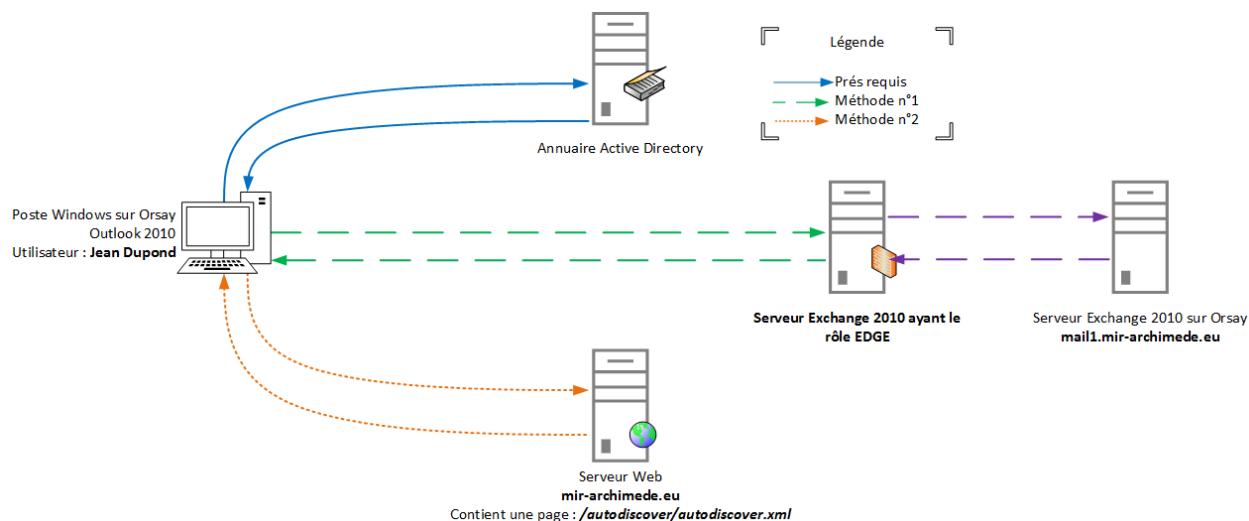
Lorsqu'un utilisateur ouvre sa session pour la première fois sur un nouvel ordinateur et lance Outlook, celui-ci tente d'utiliser chacune des cinq méthodes jusqu'à ce que l'une d'elle fonctionne. La dernière étape fonctionne forcément, car l'adresse électronique de l'utilisateur et le nom du serveur Exchange ont été récupérés pendant l'étape des prérequis. Le reste des paramètres inconnus est défini selon les paramètres standards de messagerie Exchange. Il est donc possible que les paramètres appliqués ne conviennent pas à la configuration réelle du serveur de messagerie.

Dans le cas de notre client Archimède nous retiendrons la première méthode qui est la plus complète et la plus efficace.

Cas des postes nomades :

La totalité des ordinateurs portables (postes nomades) de l'entreprise fonctionneront avec Windows 7 et le client de messagerie Outlook 2010, c'est pour cette raison que nous ne traiterons que ce cas. Toutefois, en cas de besoin ultérieur il sera parfaitement possible de mettre en place des clients de messagerie Mozilla Thunderbird 17 sur des ordinateurs portables fonctionnant avec Ubuntu 10.04.

L'auto configuration d'Outlook sur les postes nomade se fera de la même manière que pour les postes fixe ; Outlook récupérera les informations nécessaires dans Active Directory et la configuration sera envoyée par le serveur mail, la différence réside dans le fait qu'un intermédiaire viendra s'ajouter à la connexion avec le serveur de messagerie : le serveur EDGE.



Le but du serveur EDGE est d'agir comme intermédiaire entre la partie serveur mail d'Exchange 2010 et l'Internet. Son comportement est comparable à celui d'un reverse proxy pour un serveur Web.

Pour un utilisateur, le serveur EDGE ne présente aucune contrainte puisque celui-ci ne modifie pas le fonctionnement d'Exchange 2010.

Auto configuration Mozilla Thunderbird 17

Il existe dans Mozilla Thunderbird 17, quatre méthodes d'auto configuration. La première est spécifique à Mozilla Thunderbird mais les trois autres correspondent aux méthodes 2, 3 et 4 de l'auto configuration Outlook à savoir la récupération automatique un fichier de configuration sur un serveur correspondant au nom de domaine, l'utilisation d'un fichier XML déjà présent sur le poste de travail et l'utilisation de paramètre de découverte « standard ».

Pour ce qui est de la première méthode, il s'agit d'une auto configuration utilisant les paramètres standards contenus sur les serveurs de Mozilla. Cette méthode n'est utile que pour un particulier ne connaissant pas les paramètres de son fournisseur d'accès à internet, ou un prestataire de messagerie connu tel que Gmail ou Outlook.com, et n'est pas applicable dans un cadre d'entreprise.

Nous utiliserons donc la méthode numéro 2, qui est la découverte automatique d'un fichier de configuration XML grâce au nom de domaine.

Auto configuration des clients mobiles

Le client ne nous a pas donné de consigne concernant les clients mobiles, nous en déduisons que les mobiles et autres Smartphones ne seront pas professionnels.

De ce fait il est plus compliqué de prévoir la configuration de ceux-ci car sans contrôle sur les mobiles il est impossible de garantir leur fiabilité. Il existe en effet le risque d'une infection viral, mais également d'une perte ou d'un vol du terminal mobile.

Nous ne pouvons que déconseiller à notre client Archimède de courir ce risque, toutefois la décision finale ne nous revient pas, et si le client le souhaite il sera possible de fournir des procédures détaillées pour la sécurisation, et le paramétrage des clients de messagerie des principales plateformes mobiles.

Il faut tout de même noter que, comme nous le verrons plus loin, l'interface Web d'Exchange 2010 peut être utilisée sur les Smartphones récent.

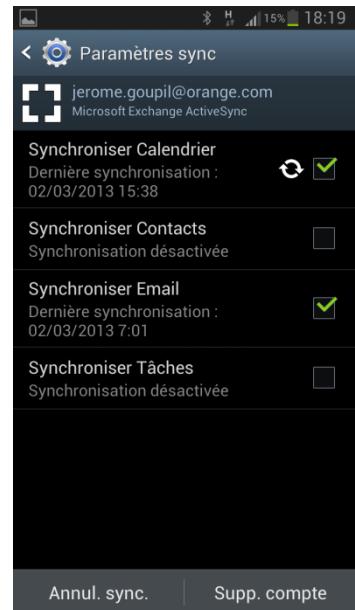
Accès à la messagerie depuis les téléphones mobile

Sur mobile et Smartphone il existe plusieurs façons d'accéder à sa messagerie Exchange 2010.

Il est d'abord possible de la consulter au travers d'Outlook Web Access mais, même si l'interface est adaptée pour la petite taille des écrans de mobile, ce n'est pas aussi pratique que sur un écran d'ordinateur. Cette interface peut être utilisée sur n'importe quel téléphone mobile disposant d'un navigateur internet récent.

On peut ensuite utiliser un client de messagerie « standard », c'est-à-dire qui ne gère que l'envoie et la réception des messages électroniques. Ces clients « standard » existent sur toutes les plateformes mobiles, même celle ayant quelque années.

Enfin, il est possible d'utiliser des clients de messageries « évolué » dans le sens où ils prennent en charge le protocole Exchange Active Sync. Ce protocole a été créé par Microsoft spécialement pour la synchronisation de la messagerie sur mobiles. Il est ainsi possible de synchroniser son calendrier, ses contacts, ses messages électroniques et ses tâches pour retrouver un client de messagerie complet sur son mobile. Le protocole Exchange Active Sync existe sur les principales plateformes mobiles récentes, Android, Windows Phone, BlackBerry et iOS.



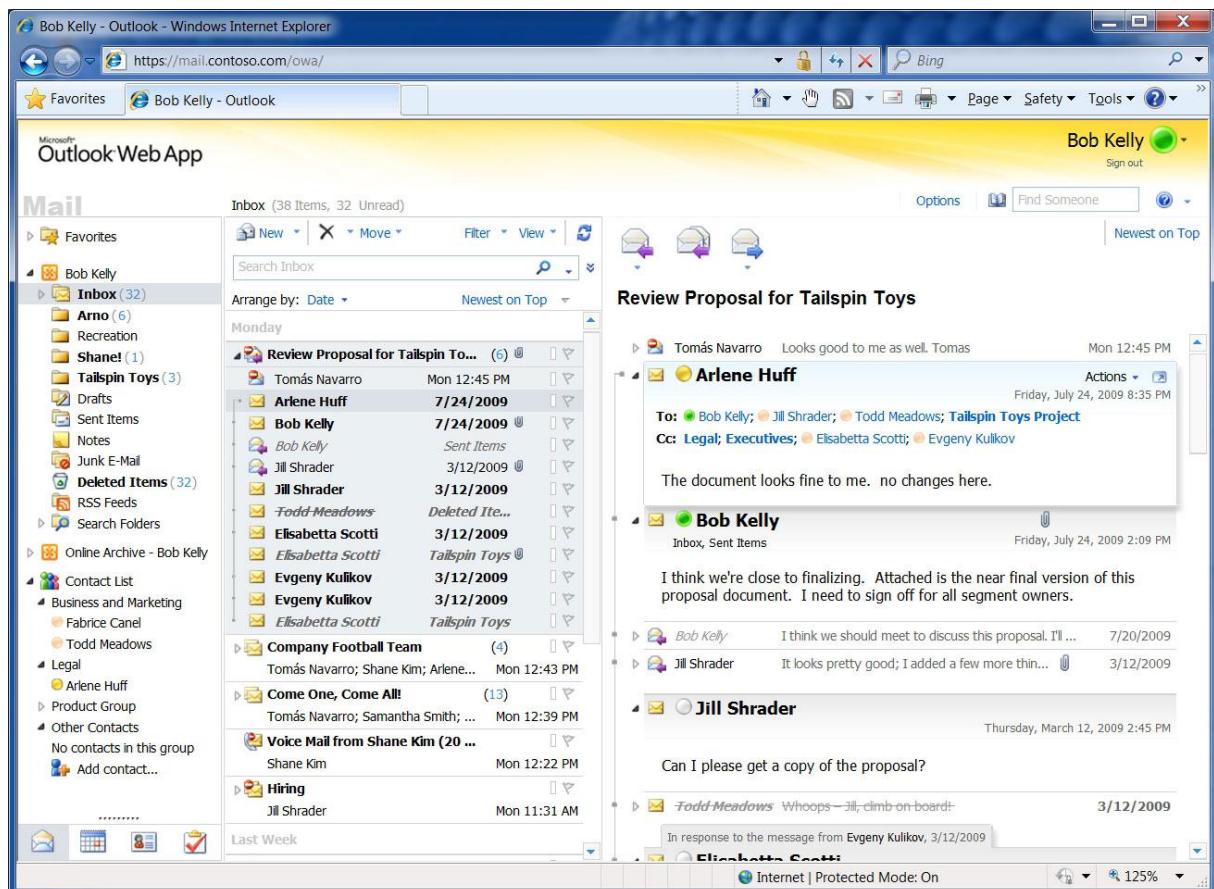
Accès à la messagerie depuis les postes nomades

Les postes nomades étant équipés d'Outlook 2010 ils bénéficieront des mêmes fonctionnalités que les postes fixes tant qu'ils seront connectés à internet. Une fois déconnecté, dans les transports en commun par exemple, Outlook passe en mode hors ligne. Dans ce mode les utilisateurs ne pourront évidemment plus envoyer de mails, créer de réunion ou réaliser toutes autres actions nécessitant la connexion au serveur de messagerie. Ils seront par contre toujours possible de consulter leurs mails et leurs réunion en lecture seul car ceux-ci seront sauvegardés en local sur les postes

Outlook permet également la création de messages électroniques lorsqu'il est en mode hors ligne. L'intérêt de cette fonction est que tous les messages créés quand Outlook est en mode hors ligne seront automatiquement envoyés lors de la récupération de la connexion internet.

Accès à la messagerie depuis un navigateur internet avec Outlook Web Access

Microsoft Exchange 2010 propose un accès à la messagerie au travers d'un simple navigateur web. Appelé Outlook Web App OWA, cette interface présente l'intérêt d'offrir la possibilité d'accéder à la quasi-totalité des fonctionnalités d'Outlook 2010 directement au sein d'un navigateur, et ceci depuis n'importe où, sur n'importe quelle plateforme et de manière sécurisée grâce au protocole SSL2/TLS qui garantit la sécurisation des échanges avec le serveur.

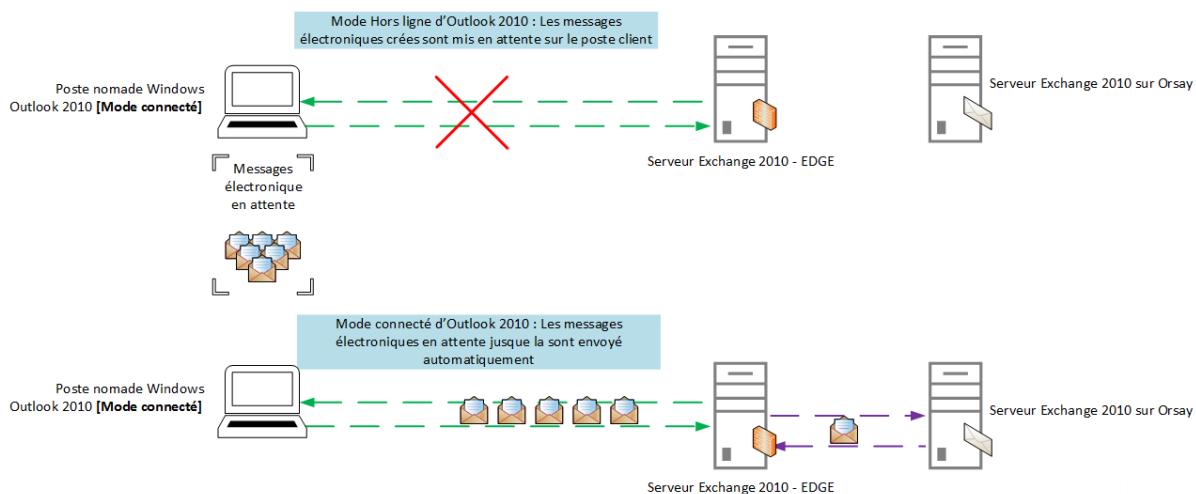


[Crédit capture d'écran : inferic.com]

Cette interface est toutefois techniquement limitée par son environnement d'exécution, à savoir le navigateur Web, et n'a pas pour fonction de remplacer le client lourd Outlook 2010, mais plutôt de le compléter.

Parmi les fonctionnalités absentes d'OWA 2010, on peut notamment citer l'import ou d'export des bases de données de mail. En effet, contrairement à un client lourd classique, une interface Web ne stocke aucune ou très peu de données en local, les mails restent donc sur le serveur de messagerie. Le multi compte est également absent, et il faudra ouvrir plusieurs instance d'OWA pour accéder à plusieurs compte de messagerie simultanément.

Outlook Web App peut bénéficier de l'authentification unique (SSO) dans le cas d'un accès depuis une session connecté sur le domaine du client Archimède.



Utilisation avec l'annuaire Active Directory

L'intégration avec l'annuaire de l'entreprise est un élément indispensable dans la mise en place d'une plateforme de messagerie électronique. Cette intégration doit permettre au minimum d'utiliser les comptes présents dans l'annuaire pour créer des comptes de messagerie électronique.

Exchange est fortement intégré dans l'annuaire Active Directory. Au lieu d'utiliser une base de données isolée comme le font la plupart des solutions du marché, Exchange modifie le schéma de l'annuaire Active Directory pour ne réaliser qu'une seule base de données unifiée pour les comptes ordinateur, utilisateur et messageries.

Cette façon de faire permet une centralisation des données dans un seul et même endroit, donc un gain important au niveau de la simplicité de gestion. Il n'est pas nécessaire de maintenir une base de données supplémentaire.

Concrètement, ce système de base de données centralisé dans le seul schéma de l'annuaire Active Directory permet à un utilisateur de faire une recherche dans ce même annuaire et de trouver, par exemple, les listes de distribution dont un utilisateur est membre, chose impossible avec les autres solutions, exceptions faites de celles proposant un connecteur dédié.

Etude des fonctionnalités de sécurité de Exchange 10

Auteur : Jérôme GOUPIL

Topologie sécurisé :

Il faut savoir que l'ensemble des serveurs Exchange ne seront pas accessibles depuis l'extérieur. Comme nous l'avons vu, seul le serveur EDGE sera accessible depuis l'extérieur car il est positionné sur la DMZ de l'entreprise. Cette logique de placement permet aux serveurs plus sensibles comme les serveurs de bases de données mail d'être protégés contre des attaques externes à l'organisation.

De même, les communications qui seront établies entre un client externe en Web mail (OWA) et Outlook via la fonctionnalité Anywhere seront sécurisé par la mise en place d'un chiffrement SSL qui garantira la sécurité des transmissions.

Sécurité contre les virus :

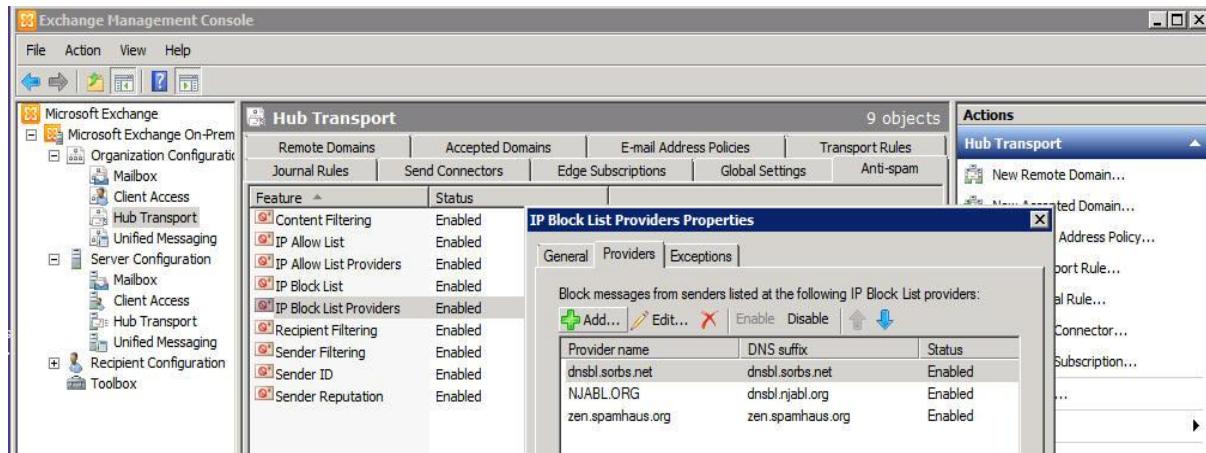
Afin de protéger votre organisation des menaces provenant d'Internet, nous équiperons les serveurs EDGE d'Archimède de la solution d'Anti-Virus Kaspersky Total Security for Business.

Issu de la suite Kaspersky End point, cette solution anti-virus analysera tous les messages entrant et sortant de l'organisation et appliquera la politique de sécurité de l'entreprise afin de contrer les Spam et virus éventuellement présents.



Protection de l'organisation contre les pourriels :

Exchange Server intègre nativement une sécurité contre les messages indésirables. Microsoft tient à jour un certain nombre de liste qui recense des éléments indésirables. Il est également possible d'exercer du filtrage par expéditeurs, destinataires etc...



Sender ID :

La technologie Sender ID est une technologie propriétaire qui consiste à vérifier que le nom de domaine source du serveur SMTP qui délivre un courrier a bien été autorisé par son administrateur. Pour vérifier le, on consultera l'enregistrement SPF (pour Sender Policy Frameworks) qui a été créé dans la zone DNS source.

L'enregistrement indique les serveurs SMTP qui sont autorisés à relayer des courriers pour un nom de domaine. Si le serveur SMTP qui envoie un courriel et qu'il n'est pas explicitement autorisé, il est possible d'indiquer au serveur Exchange de supprimer le message en question. Cela permet d'éviter les usurpations de noms de domaine (C'est une protection contre le spam).

Gestion des droits numériques :

Exchange permet par l'intermédiaire d'un service de gestion des droits nommé RMS (pour Rights Management Services) de gérer la confidentialité des informations échangées par le client Archimède.

Pour cela, il est possible de créer des règles sur le serveur HUB qui active l'utilisation des droits numériques nommé IRM (pour Information Rights Management) qui en fonction d'une politique configuré par l'administrateur sur des critères comme l'objet, le destinataire ou l'expéditeur.

Grâce à ces règles, on pourra par exemple faire en sorte qu'on ne puisse pas imprimer un message contenant un terme particulier, par exemple « Message confidentiel ».

Envoi de courriers chiffrés / signés en interne ou entre entreprises partenaires :

Exchange 2012 permet à un utilisateur d'envoyer un message signé et/ou chiffré (en utilisant le SMIME) vers un utilisateur d'une société partenaire. Au préalable, l'expéditeur devra au préalable transmettre son certificat au destinataire afin qu'il puisse déchiffrer et/ou authentifier le message.

Il existe plusieurs méthodes pour s'échanger les certificats:

- + Par courriel : l'utilisateur transmet le certificat en pièce jointe dans un message électronique
- + En utilisant un support externe : l'utilisateur utilise un périphérique pour fournir son certificat au destinataire (clé USB, carte à puce...).

Fonctionnalité de sécurité du Webmail :



Il est possible pour un utilisateur d'Archimède de se connecter par le biais d'une interface WEB sécurisé utilisant le chiffrement SSL (pour Secure Socket Layer). De plus lorsqu'un utilisateur se connecte, un cookie est utilisé pour stocker les informations d'authentification de manière chiffré le temps de la connexion. Grâce à ce cookie, le serveur exchange pourra surveiller le temps d'activité sur la session et ainsi il pourra couper la communication si l'utilisateur reste inactif trop longtemps. La durée d'expiration du cookie sera réglé en fonction de si « il s'agit d'un ordinateur public ou partagé » ou s'il s'agit d'un ordinateur privé ».

La durée d'inaktivé peut être réglée par l'administrateur.

Etude des fonctionnalités des accès / sécurité de Lync 10

Auteur : Nicolas BROISIN

Connexion automatique des clients, autoconfiguration

Pour autoriser la configuration automatique des clients à se connecter à leur session utilisateur Lync, il faut créer un enregistrement SRV DNS du serveur Lync qui distribue les demandes de connexion émises à partir des clients Lync. Cela permet d'avoir un dialogue d'authentification automatique entre le serveur Lync et l'Annuaire Active Directory.

Découverte automatique, Lyncdiscover

Lorsque vous prenez en charge la découverte automatique, vous devez ajouter de nouveaux enregistrements DNS (Domain Name System).

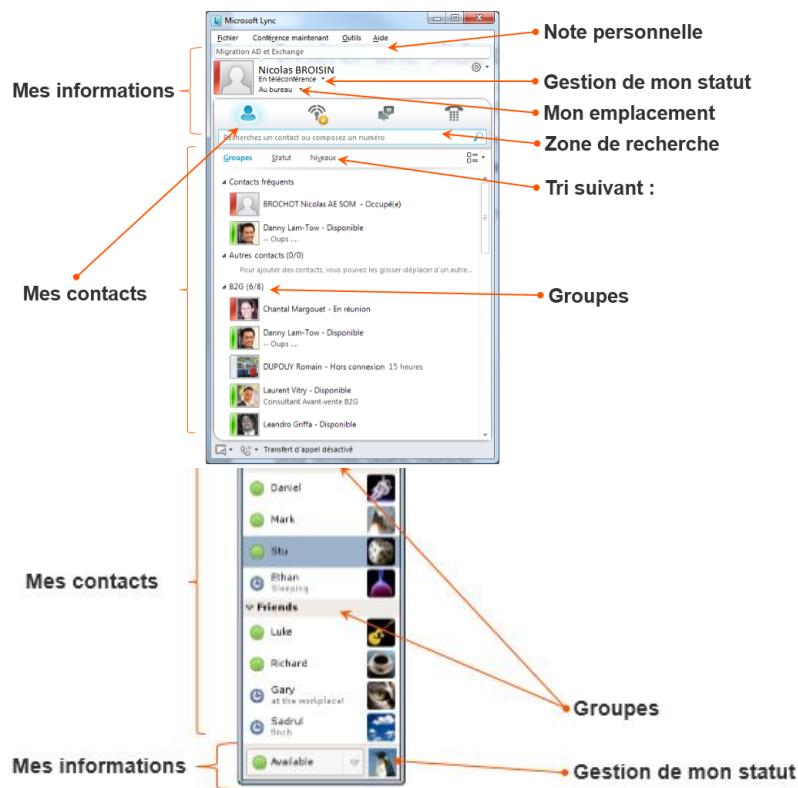
Un enregistrement DNS interne afin de prendre en charge les utilisateurs qui se connectent depuis le réseau de votre organisation ;

Un enregistrement DNS externe, ou public, afin de prendre en charge les utilisateurs mobiles qui se connectent depuis Internet.

Présentation des clients lourds : Lync 2010 et Pidgin

Client Pidgin et Client Lync 2010

Nous utiliserons le client Lync 2010 pour les postes Windows et pour les clients Linux, comme le client Lync n'existe pas, la solution Pidgin sera utilisée avec le plugin Office Communicator.



Client mobile



De plus en plus de travailleurs de l'information utilisent leur téléphone cellulaire comme seul téléphone. Les clients mobiles profitent du pouvoir que leur offrent des communications unifiées mobiles, notamment des fonctionnalités de présence enrichies, l'audioconférence et un accès à de multiples modes de communication à partir d'une interface unique et facile à utiliser.

Lync Attendee

Lync Attendee est une console permettant l'accès à une réunion Online qui peut être utilisée dans le cas où le client Lync n'est pas déployé sur le poste de travail.

Cette console peut être très utile pour permettre à des personnes extérieures d'assister à des réunions en ligne. Grâce à cette dernière, il sera possible d'avoir accès aux fonctionnalités audio et vidéo de la réunion.

Il existe 2 versions de Lync Attendee :

- Une version pour les personnes ayant les droits d'administrateur local sur leur poste de travail
- Une version pour les personnes qui ne possèdent pas de droits d'administrateur local sur leur poste de travail

Lync Web App

Lync Web App est un moyen d'accéder aux services Lync sans voir à déployer un client « lourd » sur son poste de travail. Un simple navigateur Web permettra de joindre une réunion en ligne sans avoir à installer de logiciel supplémentaire.

Toutefois, pour un organisateur désirant utiliser Lync Web App, le partage de bureau nécessitera l'installation d'un ActiveX sur son poste à la 1ère utilisation.

De plus, Microsoft Silverlight 4.0 est requis sur le poste. Il est donc conseillé de déployer ce logiciel de manière automatique afin d'éviter que l'utilisateur final ne soit sollicité pour réaliser l'installation lui-même

Note : Les fonctionnalités de voix et de vidéo ne seront pas disponibles avec le client Lync Web App.

- depuis un téléphone portable
- utilisation avec l'AD
- client multi plateforme (Linux / Windows)
- utilisation avec l'AD

Il n'est plus nécessaire de déplacer les personnes pour assister à des réunions, chacun pouvant suivre le déroulement depuis son poste de travail avec le client Lync 2010 et ce, quel que soit l'endroit où la personne se situe. Une connexion Internet et le serveur Lync Edge rendent possible ce mode d'accès pour quiconque.

Etude des fonctionnalités de gestion d'Exchange 2010

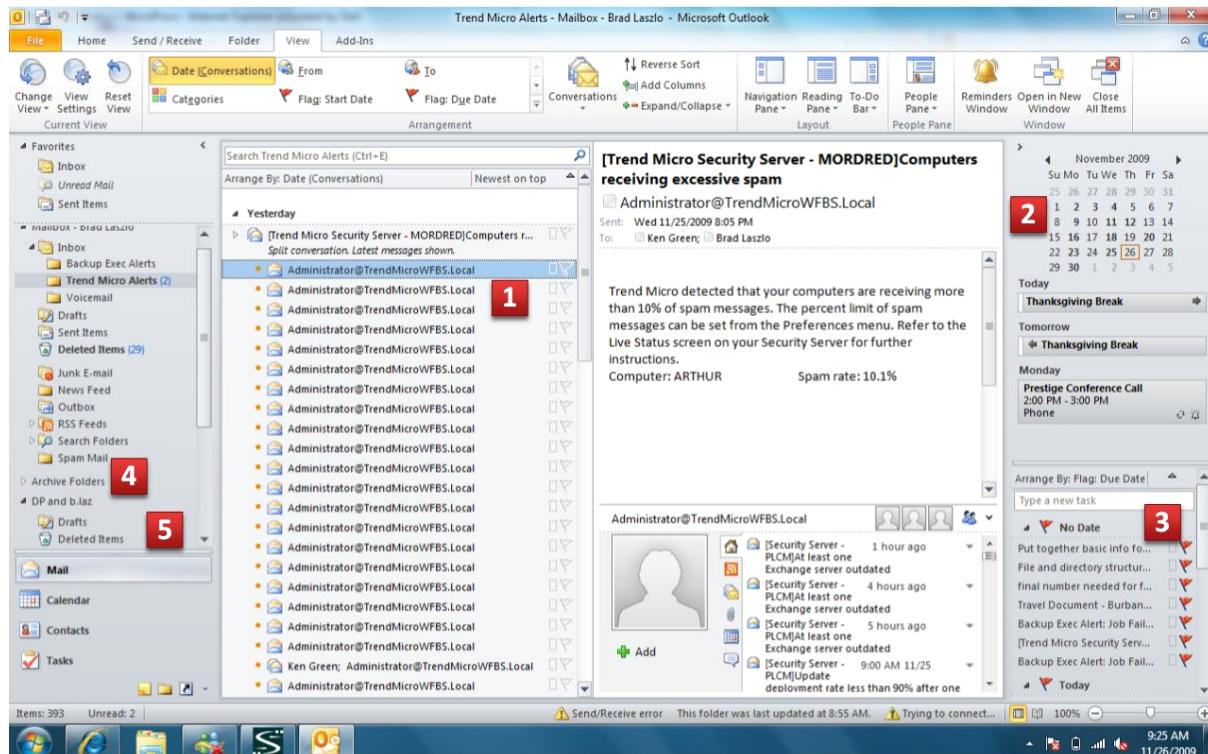
Auteur : Nicolas DOSTERT

Exchange 2010 offre nombreuse fonctionnalité. Les trois clients retenus, Outlook 2010, Thunderbird 17 et Outlook Web App sont les interfaces indispensables pour permettre aux utilisateurs d'y accéder.

Les plus importantes fonctionnalités d'Exchange 2010 sont bien sur la consultation des messages électroniques, le calendrier partagé, la liste des tâches, l'archivage en ligne et les dossiers publics.

Certaines fonctionnalités présentes dans nos clients ne sont pas liées au serveur de messagerie Exchange 2010. Ainsi le multi compte et l'archivage local dépend du client utilisé.

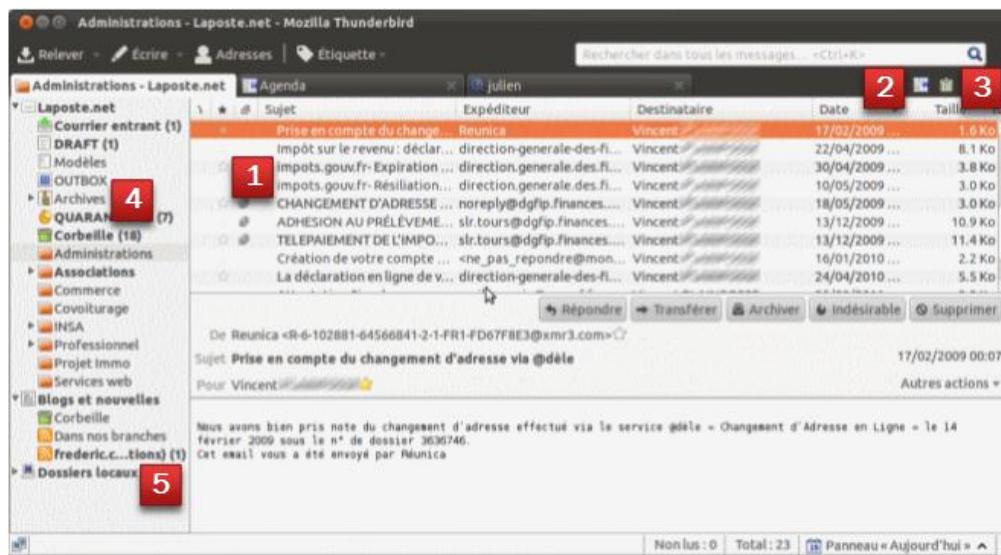
Outlook 2010 :



[Crédit capture d'écran : ptihosting.com]

1. Consultation des messages électroniques
2. Calendrier partagé
3. Liste de tâches
4. Archivage local
5. Multi-compte

Thunderbird 17 :



[Crédit capture d'écran : doc.ubuntu-fr.org]

1. Consultation des messages électroniques
2. Calendrier partagé
3. Liste de tâches
4. Archivage local
5. Multi-compte

Outlook Web App :

The screenshot shows the Microsoft Outlook Web App interface. On the left, there's a sidebar with icons for Mail (selected), Calendar (2), Contacts (3), Tasks (4), and Public Folders (5). The main area shows the inbox with several emails listed. One email is selected, showing its details on the right: "FRIDAY: Arlo Caine Math Speaker, G104 at Noon" to "everyone_list" on Wednesday, June 23, 2010, at 11:12 AM. The message body says "Friday, June 25 Goodrich 104 12:00 p.m. REU Summer Math Speaker".

[Crédit capture d'écran : wabash.edu]

1. Consultation des messages électroniques
2. Calendrier partagé
3. Liste des contacts (et messagerie instantané)
4. Liste des tâches
5. Dossiers publiques

Etude des fonctionnalités de messagerie unifiée

Auteur : Nicolas BROISIN

Lync et Exchange dialogue entre eux pour unifier la messagerie électronique, la messagerie instantanée et la téléphonie.

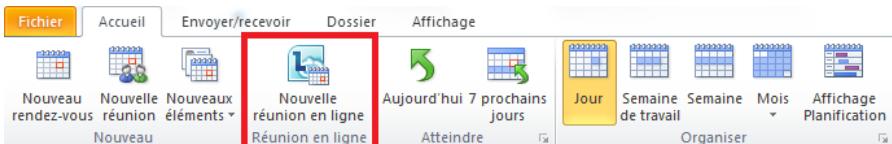
Interactions Lync et Exchange

Lync intègre de nombreuses fonctionnalités qui interagissent avec le serveur de messagerie électronique Exchange Server. Elles sont les suivantes :

- ⊕ Accès à l'historique des conversations et à la messagerie vocale
- ⊕ Lecture des messages vocaux
- ⊕ Informations sur la disponibilité et sur les heures de travail
- ⊕ Affichage de l'objet, de l'heure et du lieu de la réunion
- ⊕ Affichage d'une note et du statut d'absence du bureau
- ⊕ Synchronisation des contacts Exchange
- ⊕ Recherche des contacts personnels Outlook

Complément de conférence Lync pour Outlook

L'add-in Outlook permet la planification des réunions audio/vidéo directement depuis son calendrier Outlook. Les participants reçoivent alors un avis de réunion qui comporte un lien (URL) qui leur permettra de se connecter directement au serveur de conférence.



Cet add-in est installé automatiquement dans le client Outlook :

Pour ce qui est de la téléphonie, Lync Server utilise l'infrastructure de messagerie unifiée Exchange pour offrir les services de répondeur automatique, de notification d'appel, de standard automatique, d'accès vocal (y compris la messagerie vocale).

Répondeur automatique

La fonction de répondeur automatique lors d'un appel raté. Elle comprend la lecture d'un message d'accueil personnel, l'enregistrement d'un message et l'envoi du message au serveur de transport Hub Exchange pour qu'il soit placé en file d'attente avant d'être finalement remis à la boîte aux lettres de l'utilisateur, qui est stockée sur le serveur de boîte aux lettres Exchange.

Si un appelant laisse un message, celui-ci est transmis à la boîte de réception de l'utilisateur. Si un appelant choisit de ne pas laisser de message, une notification d'appel manqué est stockée dans la boîte aux lettres de l'utilisateur.

Outlook Voice Access

Outlook Voice Access permet à un utilisateur d'accéder non seulement à la messagerie vocale, mais également à la boîte de réception Exchange, y compris à la messagerie électronique, au calendrier et aux contacts à partir d'une interface de téléphonie. Le numéro d'accès d'abonné est attribué par un administrateur de messagerie unifiée Exchange.

Standard automatique

Le standard automatique est une fonctionnalité de la messagerie unifiée Exchange qui permet de configurer un numéro de téléphone que les utilisateurs extérieurs peuvent composer pour contacter les représentants de la société.

Services de télécopie

La messagerie unifiée Exchange comporte des fonctionnalités de télécopie, qui permettent aux utilisateurs de recevoir des télécopies entrantes dans leur boîte aux lettres Exchange.

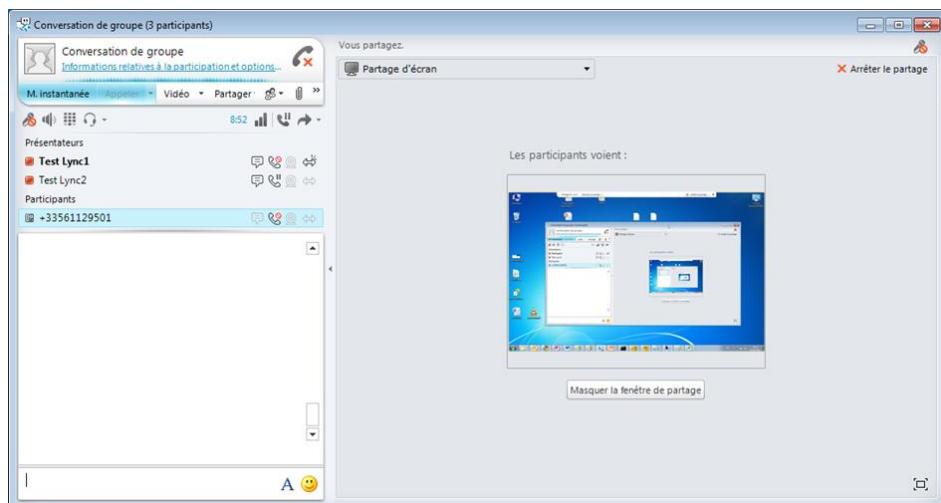
Etude des fonctionnalités de messagerie collaborative

Auteur : Nicolas BROISIN

Lync intègre plusieurs outils afin de permettre une expérience de collaboration optimisée entre salariés.

Avec Lync, le client Archimède va optimiser le **travail coopératif** de ses salariés notamment avec les nombreuses fonctionnalités de collaboration tel que la possibilité de partager des documents, de visionner un powerpoint, un tableau blanc ou encore de faire du partage de bureau et permettre de donner le contrôle à un utilisateur voulu avec un ou plusieurs utilisateurs.

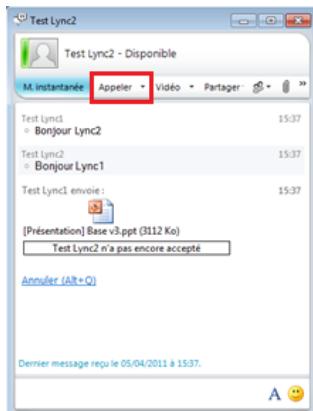
Exemple d'un partage de bureau dans le client Lync 10



Etude des fonctionnalités de visioconférence et téléphonie

Auteur : Nicolas BROISIN

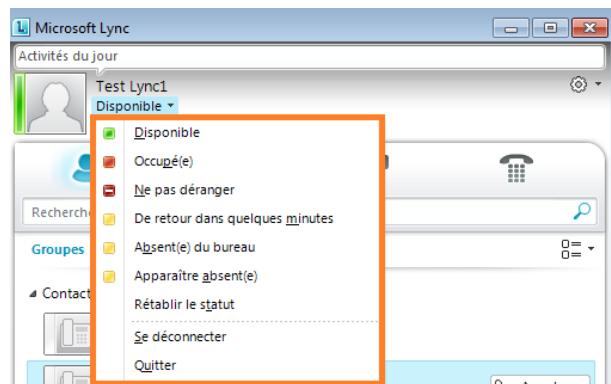
Communication en temps réel / différé



Les personnes utiliseront alors les fonctions de chat puis pourront en un seul clic continuer leur échange dans une conférence audio pour plus de convivialité ou une conférence vidéo pour partager des documents et les mettre à jour ensemble.

Indication de présence

Un point essentiel est la gestion de la présence qui permet à tous les collaborateurs de voir instantanément la disponibilité d'une personne, d'une équipe et ainsi de pouvoir entre en communication instantanément pour traiter d'un point urgent. On voit ici que la solution Lync 2010 est bien un complément à la messagerie asynchrone que nous utilisons tous depuis de nombreuses années mais le plus apporté par Lync 2010 est sa capacité à renseigner un collègue sur sa disponibilité et de mettre en contact les personnes pour qu'elles puissent communiquer par le moyen le mieux adapté à l'instant présent.



La gestion de la présence peut être :

- + Automatique : activités Lync ou rendez-vous (Outlook)
- + ou Manuelle

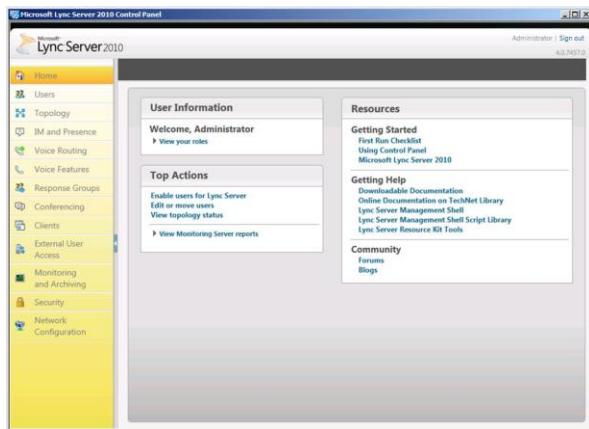
Etude des fonctionnalités d'administration Lync 2010

Auteur : Nicolas BROISIN

Topology Builder

L'outil « Topology Builder » est une des nouveautés de LYNC Server. Il permet de créer et éditer la topologie avant de déployer l'infrastructure. Cet outil permet ainsi de valider une topologie avant même de commencer l'installation des serveurs.

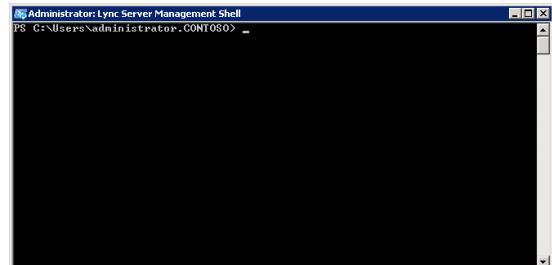
Lync Server Control Panel



Pour les tâches courantes d'administration de Lync une interface nécessaires à la gestion et à la maintenance de Lync Server 2010. Pour plus d'informations sur les tâches d'administration que vous pouvez effectuer par le biais du Panneau de configuration Lync Server 2010, voir Panneau de configuration Lync Server.

Microsoft Lync server 2010 Powershell

Il faut savoir que le Powershell est très utilisée pour automatiser certaines tâches d'administration. Il offre une nouvelle méthode d'administration et de gestion. Lync Server Management Shell est une puissante interface de gestion reposant sur interface de ligne de commande Windows PowerShell, qui inclut un jeu complet d'applets de commande spécifiques à Lync Server 2010. Avec Lync Server Management Shell, vous disposez d'un ensemble complet de commandes de configuration et d'automatisation.



Lync Attendant Console

Lync Attendant console est optimisée pour les délégués et autres utilisateurs chargés de traiter un grand volume d'appels, tels que les réceptionnistes et offre une interface utilisateur en mode plein écran pour une gestion des appels efficace.

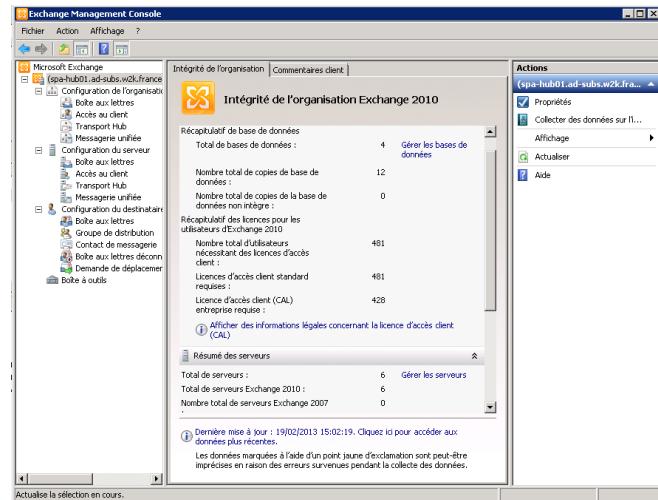
Lync Attendant console permet de recevoir et de transférer des appels pour et vers n'importe qui au sein de l'entreprise, en fonction de son état de présence. La section de conversation, avec une mise en file d'attente automatique des appels entrants, actifs et en attente, permet aux utilisateurs de gérer plusieurs conversations en même temps et la section des contacts peut être personnalisée par les utilisateurs pour une efficacité maximale.

Etude des fonctionnalités d'administration Exchange 2010

Auteur : Jérôme GOUPIL

L'administration d'Exchange peut se faire de deux manières :

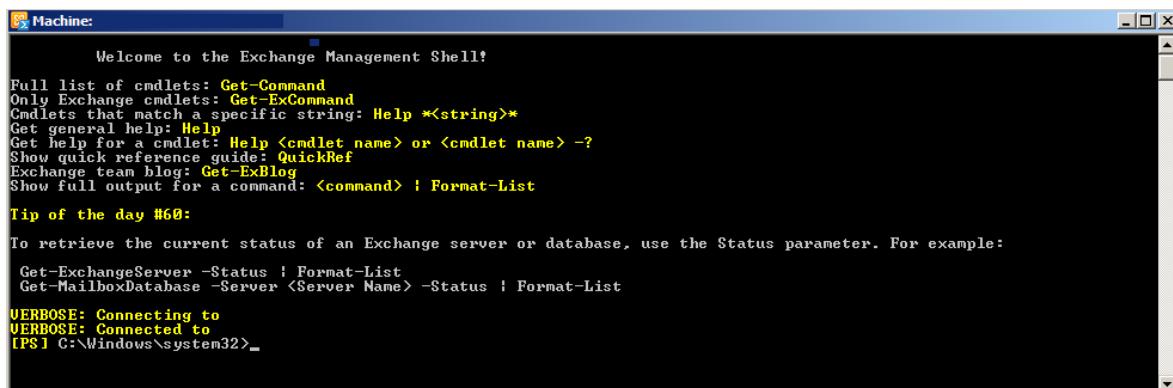
- ✓ via l'interface graphique Exchange Management Console (EMC)



- ✓ via la console Exchange Management Shell (EMS).

L'interface EMC permet de lancer de nombreux outils et de lancer de nombreuses tâches d'administration en mode graphique.

L'interface EMS quant à elle apporte de nombreuses commandes supplémentaires dédiées à l'administration des services de messageries. Toutes les fonctionnalités clés de Windows Power Shell sont supportées. De nombreuses manipulations ne sont pas réalisables via l'interface graphique et doivent être exécuté via ce Shell.



```

Machine: Welcome to the Exchange Management Shell!
Full list of cmdlets: Get-Command
Only Exchange cmdlets: Get-ExCommand
Cmdlets that match a specific string: Help <string>
Get general help: Help
Get help for a cmdlet: Help <cmdlet name> or <cmdlet name> -?
Show quick reference guide: QuickRef
Exchange team blog: Get-ExBlog
Show full output for a command: <command> | Format-List

Tip of the day #60:
To retrieve the current status of an Exchange server or database, use the Status parameter. For example:
Get-ExchangeServer -Status | Format-List
Get-MailboxDatabase -Server <Server Name> -Status | Format-List

VERBOSE: Connecting to
VERBOSE: Connected to
[PS] C:\Windows\system32>_

```

Déploiement de la solution

Architecture logique de Lync 10

Auteur : Nicolas BROISIN

Les différents rôles que l'on va implémenter

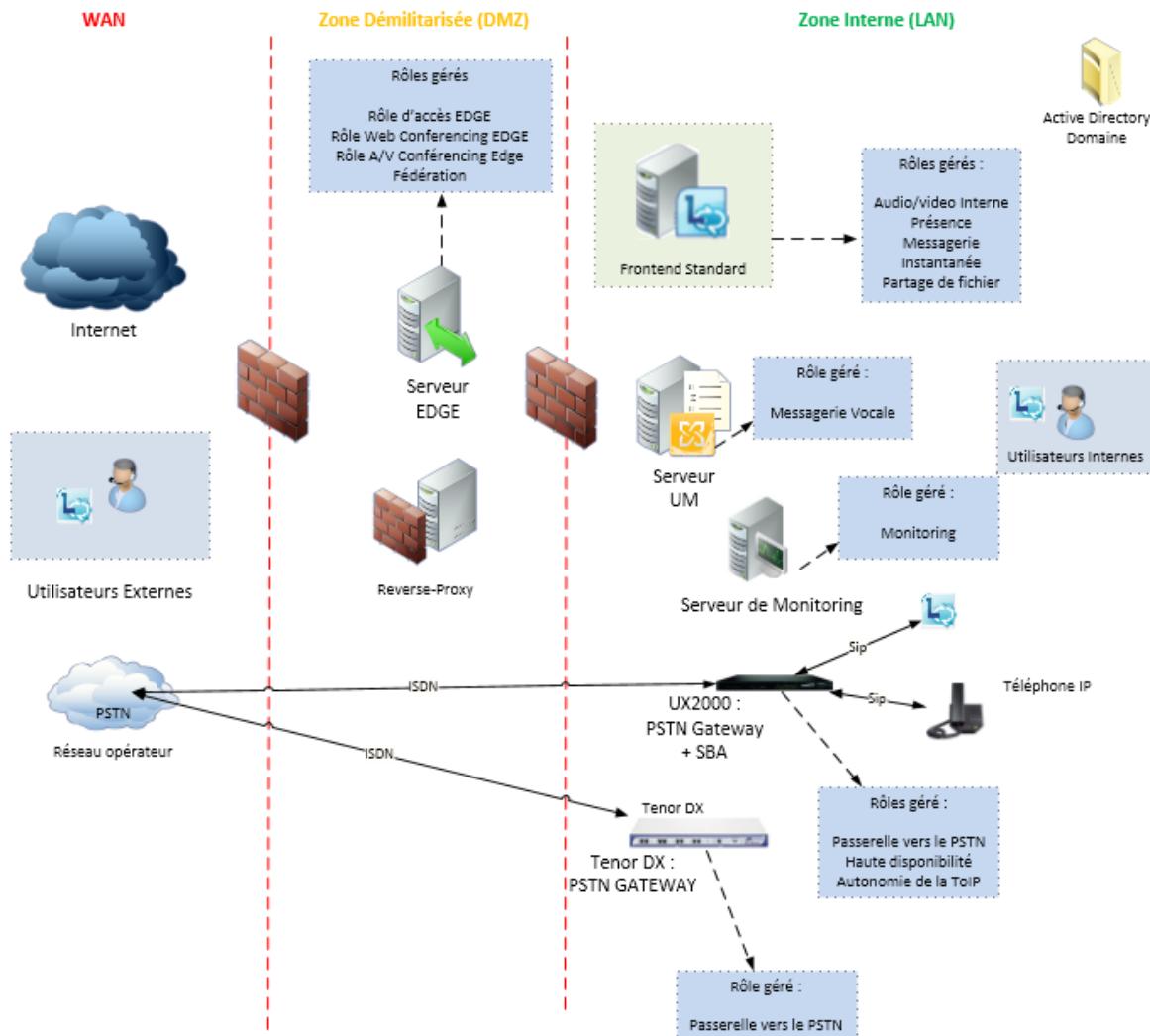
Voici une liste des principaux rôles fournis par Lync Server 2010. Ces rôles sont répartis en deux thèmes :

- Rôles proposés pour une utilisation interne à l'entreprise
- Rôles proposés pour une utilisation externe à l'entreprise

➔ Voir en annexe la description des rôles.

Cette architecture permet de gérer l'ensemble des rôles et services Lync de manière fonctionnelle. Nous distinguerons donc une infrastructure à 3 niveaux :

- Niveau Interne (LAN)
- Niveau périmètre (DMZ)
- Niveau Externe (Internet)



Concrètement voici le schéma d'architecture logique proposée pour le client Archimède :

→ **Voir la topologie logique de Lync en annexe 9 (page 70)**

Architecture physique de Lync 10

Auteur : Nicolas BROISIN

Comme indiqué dans le schéma de l'architecture logique, la plateforme Lync Server 2010 est conçu de manière à pouvoir s'adapter à la fois à la croissance de l'entreprise, à des besoins spécifiques comme les besoins de communications téléphonique avec l'extérieur.

Pour cela, l'architecture Lync Server 2010 est constituée des différents rôles (détaillés dans la partie Architecture logique) et offre ainsi une infrastructure évolutive, sécurisée et tolérante aux pannes si besoin. Grâce à la modularité de la plateforme Lync il sera possible de compléter les fonctionnalités au fur et à mesure que le besoin se manifestera au sein de l'entreprise ou avec l'extérieur de l'entreprise.

Les différentes architectures possibles

L'architecture d'une solution varie en fonction de nombreux critères notamment suivant la version de la solution. Dans notre cas Lync 2010 propose 2 possibilités d'architecture, une version Enterprise et une version Standard.

Version Enterprise

Microsoft Lync Server 2010, en édition Enterprise, permet les déploiements à grande échelle adaptés aux grandes entreprises. **L'architecture peut ainsi supporter une charge de 5000 à 125 000 utilisateurs.**

Cette solution est principalement conçue pour la redondance et la haute disponibilité. Les serveurs sont déployés sous forme de pool, derrière un système d'équilibrage de charge matériel (HLB – Hardware Load Balancer).

Version standard

Lync Server 2010 est également disponible en version Standard mais cette dernière est plutôt adaptée à des scénarios où la tolérance de pannes n'est pas requise en sachant que **le nombre d'utilisateurs est de 5000 maximum par serveur.**

Lync Server 2010 Standard est un serveur autonome où tous les rôles sont installés localement en plus de la base de données SQL.

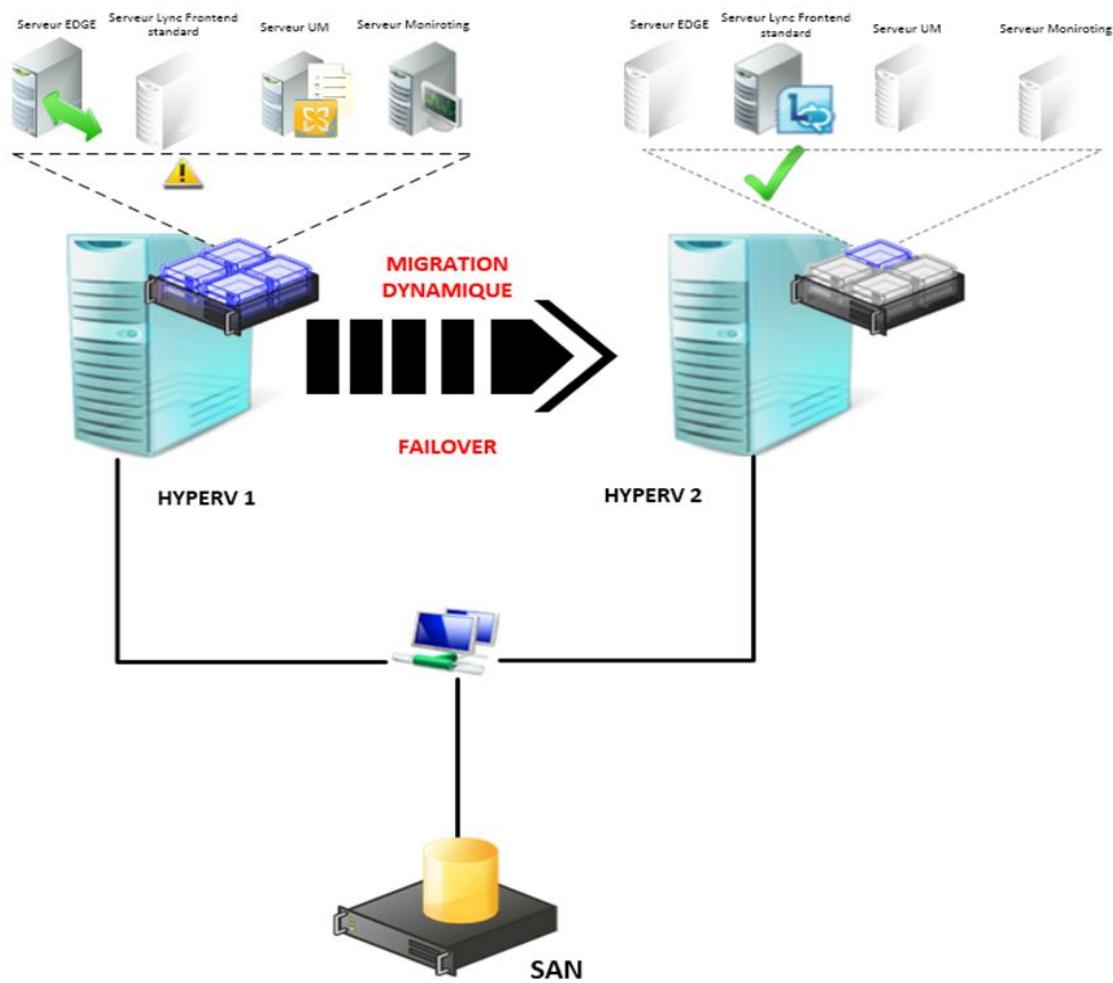
Notre choix d'architecture

Le choix de la version sera axé sur une version Standard car la redondance du SQL Mirroring est un investissement très cher et pas recommander dans notre cas avec moins de 1000 collaborateurs en totalité. En effet, il faut savoir que pour le SQL Mirroring il faut minimum 2 serveurs SQL ce qui demande 2 serveurs très performant et pour ce qui est des licences SQL server elles sont très onéreuses.

Enfin, pour la haute disponibilité nous allons opter pour la virtualisation des serveurs. Si le nœud tombe, une copie ailleurs prendra le relai manuellement ou automatiquement via script.

Nous allons profiter de notre parc informatique entièrement Windows pour mettre en place un nœud de cluster Hyper-V pour faire de la haute disponibilité au niveau de la couche virtualisation. Nous allons les relier à un stockage partagée de type SAN.

En effet, La migration dynamique est une fonctionnalité de Hyper-V dans Windows Server 2008 R2. La migration dynamique permet de déplacer de façon transparente des ordinateurs virtuels à partir d'un nœud du cluster de basculement vers un autre nœud du même cluster, sans interruption de la connexion réseau ou perception d'un temps mort. En outre, le clustering avec basculement requiert des stockages partagés pour les nœuds du cluster, ce qui peut inclure un protocole iSCSI ou Fiber-Channel SAN.



Récapitulatif de l'architecture physique :

Serveurs	Rôles	Virtualisé	Emplacement
Serveur EDGE / Reverse proxy	<i>EDGE – Accès Externes</i>	Oui	DMZ
Serveur Lync Standard Front-End	<i>Front-End - Pool</i>	Oui	Interne
Serveur de Monitoring	<i>Surveillance QOE, stats.</i>	Oui	Interne
GW NET UX2000	<i>Téléphonie Opérateur</i>	Non	Interne
GW NET Tenox DX	<i>Téléphonie Opérateur</i>	Non	Interne
Serveur UM	<i>Messagerie Vocale</i>	Oui	Interne

→ Voir la topologie physique de Lync en annexe 10 (page 71)

Explication de l'architecture

Voici les spécifications des différents serveurs énumérés dans le tableau ci-dessus :

Le Serveur Edge :

Le serveur EDGE doit être dans la zone Démilitarisée. C'est lui qui va permettre les accès externes (Fédération, Web conférence, etc.).

C'est ce serveur qui fera office de Reverse-Proxy ou proxy inversé.

Il remplira le rôle de passerelle entre Internet et le réseau local. Il donne accès depuis l'extérieur et via Internet aux serveurs internes de l'entreprise en transmettant indirectement les requêtes qui lui sont adressées. Cela évite à l'entreprise de trop exposer ses serveurs Web frontaux, en les plaçant derrière un serveur sécurisé et prévu pour encaisser des grosses charges de trafic.

Dans le cadre de Lync, le Reverse Proxy va permettre d'authentifier les utilisateurs externes (principalement.) sur les services suivants :

- ⊕ Dialin
- ⊕ Web conférence externe (Via URL)
- ⊕ Lync Mobile.

Le serveur Lync 2010 Standard Front-End :

Ce serveur doit être dans la zone interne, ainsi que dans le domaine Active Directory En effet, c'est le serveur qui va gérer le pool principal de l'infrastructure Lync. Il embarque un serveur SQL express et possède un CMS (Central Management Store) contenant les propriétés de la topologie. 7

Le serveur UM

Ce serveur sera également dans le domaine, ainsi que dans le LAN. C'est lui qui va gérer la notion de messagerie vocale sur la partie Lync.

Le serveur de monitoring

Ce serveur doit être dans la zone interne, ainsi que dans le domaine. Il va permettre la mise en place de surveillance et de statistiques sur l'infrastructure Lync Server 2010.

Partie téléphonie IP

Une solution VoIP à l'échelle de l'entreprise doit de toute évidence assurer l'acheminement des appels depuis et vers le réseau téléphonique commuté (PSTN) avec une qualité de service constante. En outre, la technologie sous-jacente doit être transparente pour les utilisateurs lorsqu'ils passent ou reçoivent des appels. De leur point de vue, un appel entre l'infrastructure Voix Entreprise et le RTC doit ressembler à toute autre session SIP.

Le choix s'est porté sur des passerelles PSTN plutôt que sur du PABX beaucoup plus coûteux en termes d'acquisition et de maintenance.

Les passerelles PSTN ou (Gateway PSTN) sont des périphériques tiers qui traduisent la signalisation et le trafic multimédia entre l'infrastructure Voix Entreprise et un opérateur téléphonique (PSTN) ou un PBX (autocommutateur téléphonique privée).

La passerelle Net Tenor DX

La passerelle Net Tenox DX est une simple passerelle compatible avec l'infrastructure Lync. Elle est située sur le site d'Orsay en complément du Frontend qui permet de traduire le flux numérique venant du Frontend en signal analogique vers le réseau opérateur téléphonique (PSTN). Elle est moins coûteuse que la passerelle UX2000 qui intègre en plus le rôle de continuité de service.

La passerelle NET UX2000 avec Rôle SBA

La passerelle UX2000 du constructeur NET est une passerelle média compatible Lync permettant de faire de la téléphonie sur IP grâce à une interconnexion avec le réseau opérateur.

Comme nous l'avons cité plus haut, le serveur de médiation fait la transition entre le monde Lync et le monde IP. C'est par son intermédiaire que les conversations audio, vidéo transitent entre la Passerelle et le monde Lync. Il utilise une signalisation en G711 ne tolérant pas d'erreur. Dans notre cas le serveur de médiation est embarqué dans notre passerelle avec le SBA. C'est la raison pour laquelle nous préconisons son installation intégré dans la passerelle dans le cas des sites distants et sur le frontend dans le cas du site principal. Le SBA est un Windows 2008 server optimisé pour Lync, c'est en quelque sorte un petit frontend.

Le rôle SBA intégré à la passerelle média utilisera le rôle de médiation et sera le point de « Registrar » des utilisateurs qui se situeront chaque site distant du client Archimède.

Le rôle de registrar (Point d'enregistrement) est le point d'entrée des utilisateurs qui ont Lync activé, et pour lesquels le pool par défaut est basé sur l'UX 2000.

Cette technologie utilisée par un SBA permet de gérer de la résilience de site. En effet, en cas de coupure du lien WAN vers le Front-End, les utilisateurs ne perdront pas la téléphonie sur le site distant. (Partie collaborative en revanche, non sauvegardée durant la coupure WAN.)

Complément téléphonique : offre BTIP

Dans la téléphonie classique, il est nécessaire de passer par un PABX c'est-à-dire un autocommutateur téléphonique privé (souvent désigné par l'anglicisme Private Automatic Branch eXchange) qui coûte excessivement chère.

Grâce à la ToIP il est possible d'éviter l'acquisition d'un PABX pour effectuer des appels vers l'extérieur en souscrivant à une offre BTIp.

BTIp (en anglais Business Talk Ip) est une offre d'OBS permettant de relier différents sites d'une entreprise équipés en ToIP via un réseau WAN commun, et d'assurer la passerelle avec le réseau RTC au plus proche de la destination de façon à réduire le coût des communications externes.

Architecture logique d'Exchange 10

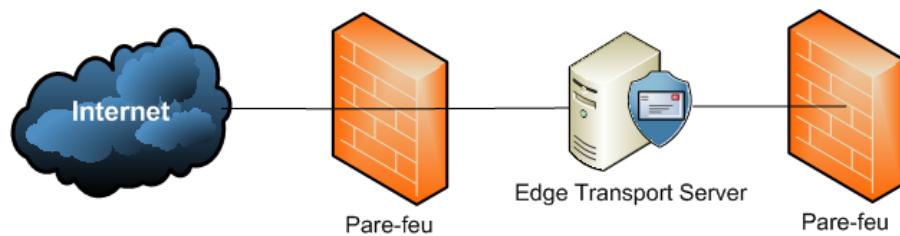
Auteur : Jérôme GOUPIL

Tout comme les précédentes versions, Exchange 2010 intègre une notion de « rôle ». Cette philosophie permet une meilleure répartition et un meilleur dimensionnement de l'architecture. Ces différents rôles peuvent être implémentés sur des différents serveurs physiques ou sur le même serveur à l'exception du rôle serveur de transport Edge.

Petit tour des différents rôles existants :

- ✓ Le rôle du serveur de transport Edge (Edge transport)

Ce rôle « tête de pont » sera placée sur la DMZ de l'entreprise et sera indépendant d'Active Directory pour des raisons évidentes de sécurité. Il s'agit d'une passerelle email qui peut accepter les courriels provenant d'Internet, ou de serveurs d'organisations externes clairement identifiés. Ce serveur va pouvoir filtrer les SPAM et Virus présents dans un message grâce à l'Anti-Virus Kaspersky Total Security for Business. Les emails entrants ayant passé l'hygiène de messagerie (c'est-à-dire les réglés définie par l'administrateur) seront routés vers les serveurs Transport Hub de l'organisation. Ce rôle ne peut pas être associé avec d'autres rôles d'Exchange.



- ✓ Le rôle serveur de boîtes aux lettres (Mailbox)

Comme son nom l'indique, ce rôle héberge les boîtes aux lettres de chaque utilisateur Exchange. Il héberge également les carnets d'adresses et permet la planification de réunions et la gestion des ressources associées. Il gère également les accès aux clients de messagerie utilisant le protocole MAPI (Messaging Application Programming Interface) qui est le protocole propriétaire de Microsoft pour les accès aux boîtes aux lettres.

- ✓ Le rôle serveur d'accès client (CAS)

Ce rôle va permettre aux clients d'accéder à leur compte Exchange. Cela comprend tous les accès non-MAPI par l'intermédiaire d'un client Outlook, de l'Outlook Web App, ou bien par Outlook AnyWhere, POP3, IMAP et ActiveSync.

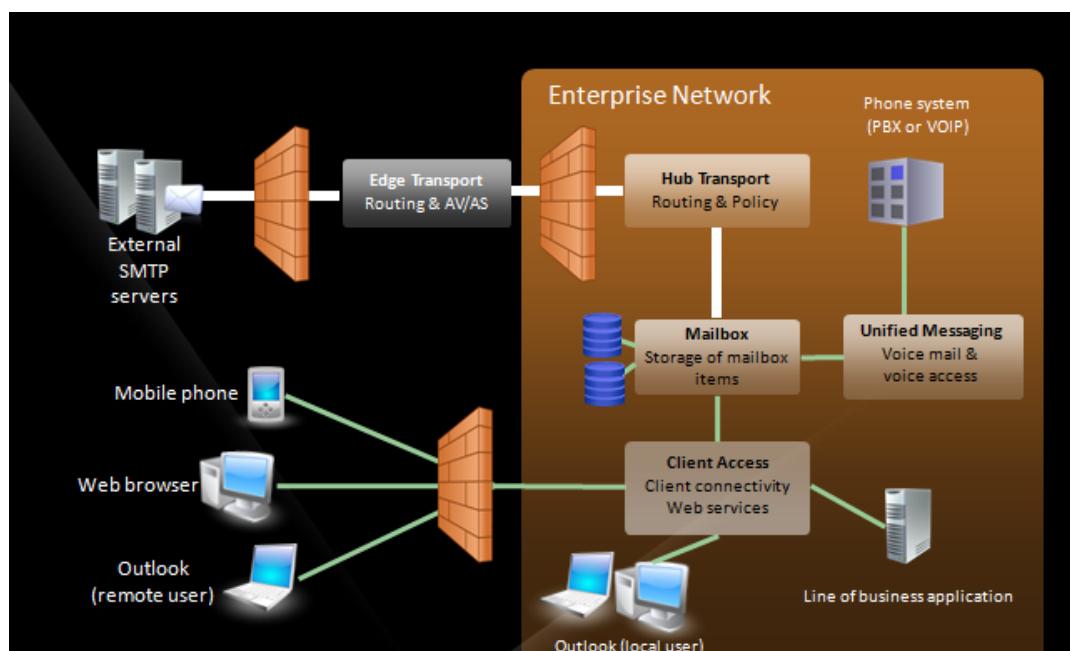
- ✓ Le rôle serveur de transport Hub (Hub transport)

Ce rôle gèrera le routage et la remise des messages dans l'organisation Exchange. Il gère également la transmission de messages en dehors de l'organisation. Il peut également effectuer un filtrage ou appliquer des règles de routage configurées par l'administrateur. Le serveur de transport peut également journaliser les messages ce qui permet d'être en conformité par rapport aux différentes réglementations en vigueur.

- ✓ Le rôle de messagerie unifiée (UM)

Ce rôle est un rôle intermédiaire permettant de lier le serveur Exchange à d'autres services de communication afin de permettre par exemple de recevoir des messages vocaux et fax dans la boîte aux lettres de l'utilisateur. Il peut également permettre la consultation d'Exchange à partir d'un téléphone.

Voici un schéma récapitulatif des différents rôles :



➔ Voir la topologie logique d'Exchange en annexe 7 (page 68)

Architecture physique d'Exchange 10

Auteur : Jérôme GOUPIL

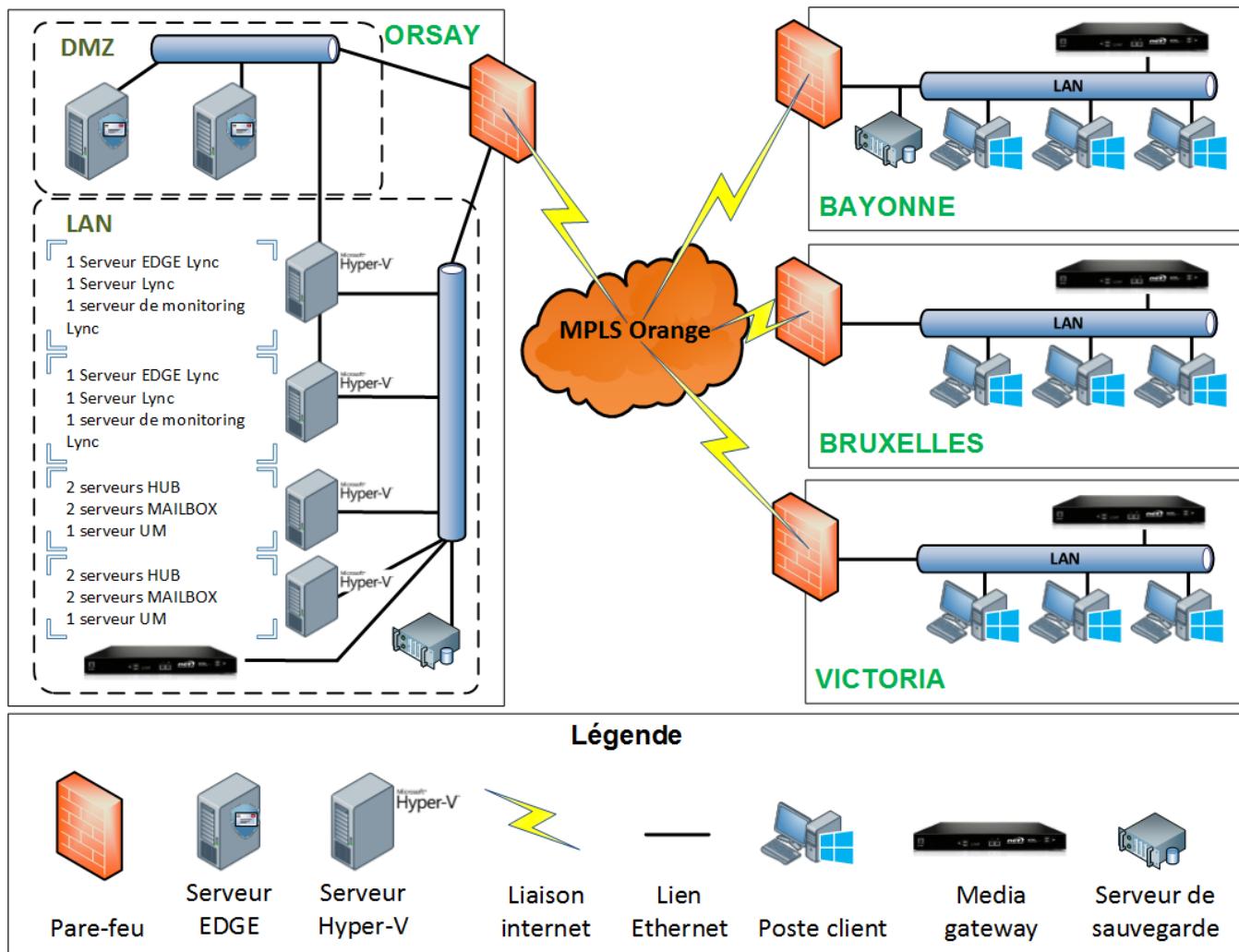
Détail sur la mise en place de l'architecture :

Dans le but d'assurer une tolérance à la panne, chaque serveur sera doublé afin d'assurer une continuité de service en cas de panne. Cela permettra aussi de bénéficier une répartition de la charge entre les différents serveurs qui seront présents dans l'architecture. De plus, les serveurs et les bases de données seront sauvegardé à deux endroits différents (Orsay et Bayonne) ce qui sécurise le client en cas d'avarie. La sauvegarde sera réalisée sur bandes magnétiques.

→ Voir la topologie physique d'Exchange 10 en annexe 8 (page 69)

Architecture physique globale

Auteur : Nicolas DOSTERT



Planification du projet

Auteur : Nicolas DOSTERT

1. Etude :

L'étude a été le moment où nous avons analysé le cahier des charges afin de cerner les besoins explicites et implicites du client. Nous avons ensuite réalisé l'étude en deux parties, une première partie dans laquelle nous avons succinctement présenté les principales solutions du marché et une deuxième partie dans laquelle nous avons détaillé techniquement les deux solutions les plus adaptées au besoin du client.

2. Installation et configuration des serveurs Exchange 2010 :

Durant cette phase nous allons installer le système d'exploitation Windows Server 2008 R2 Entreprise sur les machines physiques et virtuelles de notre infrastructure qui hébergeront les rôles Exchange 2010. Puis nous installerons les prérequis et les rôles Exchange 2010 nécessaires sur les différentes machines.

3. Installation et configuration des serveurs Lync 2010 :

Durant cette phase nous allons installer le système d'exploitation Windows Server 2008 R2 Entreprise sur les machines physiques et virtuelles de notre infrastructure qui hébergeront les rôles Lync 2010. Puis nous installerons les prérequis et les rôles Lync 2010 nécessaires sur les différentes machines.

4. Configuration des clusters :

La configuration des clusters est l'étape pendant laquelle nous mettrons en place les différents systèmes de répartition de charges et de tolérance à la panne.

5. Phase de tests :

La phase de test nous permettra de vérifier le bon fonctionnement de chaque composant de l'infrastructure. Nous vérifierons le fonctionnement de chacun des rôles d'Exchange 2010 et de Lync 2010 mais testerons également les mécanismes de répartition de charge et de tolérance à la panne.

6. Installation des clients :

L'installation des clients nous permettra de déployer les clients lourds Outlook 2010 et Thunderbird 17 afin de permettre au client de commencer la mise en production de son système de messagerie unifié.

7. Vérification Au Bon Fonctionnement :

Enfin, la vérification au bon fonctionnement va permettre de vérifier directement avec le client si toutes ses attentes ont bien été respecté et lui permettra de constater le bon fonctionnement de son infrastructure de messagerie unifiée.

→ Voir en Annexe 11 le planning du projet (page 72)

Le planning présenté en annexe vous présente les différentes étapes du déploiement et de leurs durées. La durée totale du déploiement sera de 90 jours

Coût de la solution Exchange 10 et Lync 10

Coût de la solution Exchange 2010

→ Voir en annexe 13 complément des coûts licences serveur et CAL (page 74)

Besoins matériel :

→ Voir en annexe 12 le détail (page 73)

Tableau récapitulatif des couts :

Coût des licences	Description	Prix unitaire	Quantité	Prix
DELL PowerEdge R520	Serveur de virtualisation	3700 €	2	7 400 €
DELL PowerVault MD3200i	Serveur de stockage	7 070 €	2	14 140 €
DELL PowerVault TL2000	Serveur d'archivage	11 180 €	2	22 360€
Windows Server 2008 R2 Standard	Système d'exploitation	750 €	7	5 250 €
Exchange Server 2010 Standard Edition	Système de messagerie	700 €	7	4 900 €
Kaspersky Security for Mail Server	Anti-virus de messagerie	/	pour 920 boîtes	16 000 €
Licence CAL Exchange server 2010 Premium	Licence d'accès client	89€	820 + (100 en prévision)	81 880 €
Total				151 930€

Coût de la solution Lync 2010

Auteur : Nicolas BROISIN

Dans de nombreuses entreprises, le déploiement de la solution Lync 2010 a permis d'améliorer la productivité des collaborateurs qui ont vu dans ces nouveaux outils une manière beaucoup plus rapide de communiquer entre collègues, d'échanger des informations et de travailler en commun sur des projets.

→ Complément des couts des licences serveur et CAL en annexe 14 (page 75)

Tableau récapitulatif des coûts de l'architecture proposée :

Coût des licences	Description	Prix unitaire	Quantité	Prix
DELL PowerEdge R520	Serveur de virtualisation	3700 €	2	7 400 €
Windows Server 2008 R2 Enterprise	Système d'exploitation	3 000 €	2	6 000 €
Windows Server 2008 R2 Standard (VM)	Système d'exploitation	750 €	3	2 250€
Lync 2010 Standard Edition	Système de messagerie instantanée	700 €	1	3 500 €
NET Tenor DX	Passerelle PSTN	1 500 €	1	1 500 €
NET UX 2000	Passerelle PSTN + SBA	3 000 €	3	9 000 €
Licence CAL Enterprise Lync server 2010	Licence d'accès client	135€	820 + (100 en prévision)	121 440 €
Licence Client Lourd Lync 2010	client lourd	30 €	632 postes Windows	18 960 €
Total				170 050€

Total coût Lync et Exchange :

Coût Exchange	170 050€
Coût Lync	151 930€
TOTAL	321 980

CONCLUSION

Le résultat final d'un déploiement de messagerie unifiée à l'échelle de l'entreprise est un retour sur investissement significatif. Il contribue à un certain nombre d'améliorations qualitatives dues à une meilleure collaboration et à une meilleure participation.

LEXIQUE

Cluster : Regroupement de plusieurs ordinateurs physiques afin de permettre une gestion unique, et de rassembler les performances

DMZ : Sous réseau informatique séparé du réseau local d'entreprise, afin de regrouper les serveurs accessibles depuis Internet.

IMAP : est un protocole qui permet de récupérer les courriers électroniques déposés sur des serveurs de messagerie. Son but est donc similaire à POP3, l'autre principal protocole de relève du courrier.

MAPI : est un ensemble de fonctions propriétaires, développées par Microsoft qui sont utilisées par des applications de messagerie électronique.

Pare-feu: Logiciel ou matériel garantissant la sécurité d'un réseau informatique en filtrant les paquets entrant.

PBX : Un PBX (souvent désigné par l'anglicisme PABX : Private Automatic Branch eXchange) est un autocommutateur téléphonique privé. Il sert principalement à relier les postes téléphoniques d'un établissement avec le réseau téléphonique public. On peut lui relier des équipements analogiques ou numériques.

POP3 : est un protocole qui permet de récupérer les courriers électroniques situés sur un serveur de messagerie électronique.

PRA : Plan de reprise d'activité.

RC2 : Algorithme de chiffrement dont le développement a été sponsorisé par Lotus.

SIP : Session initiation protocol est un protocole de la couche applicative qui est utilisé pour ouvrir ou fermer des sessions de télécommunications multimédia, pour la téléphonie sur IP, de la visiophonie, de la messagerie instantanée ...

SPF : est une norme de vérification du nom de domaine de l'expéditeur d'un courrier électronique, normalisé dans la RFC 4408. L'adoption de cette norme est de nature à réduire le spam.

SRTP : Protocole sécurisé de transport de donné ayant des contrainte temps réel.

T.120 : Ensemble de normes utilisé pour les conférences et les échanges de données multipoints.

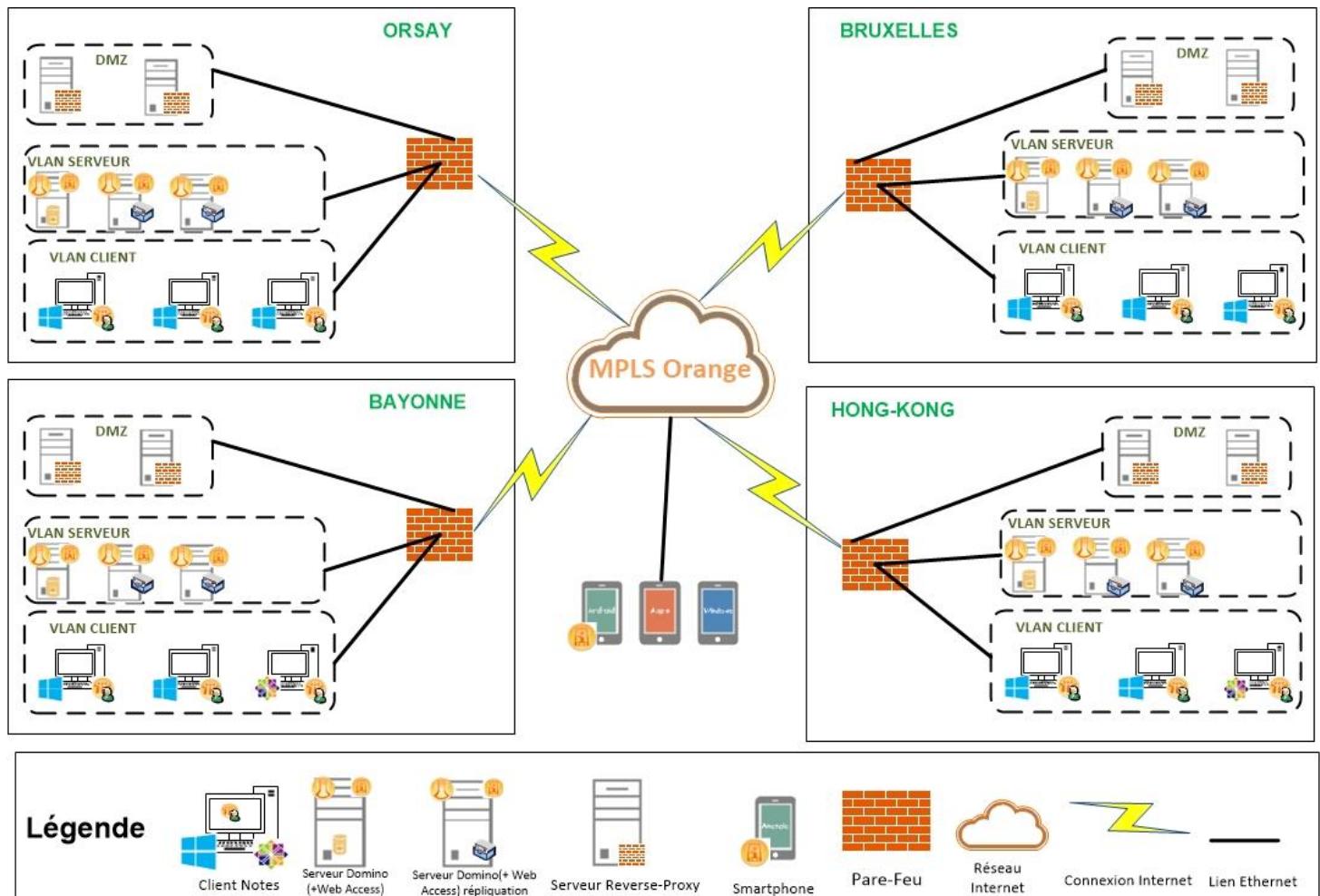
TLS : Protocole standardisé de sécurisation des échanges

Token : Information obtenu après authentification permettant l'accès au différent service.

VoIP : Voice over IP, est une technique qui permet de communiquer par la voix ou audio/vidéo sur des réseaux IP privés ou publiques, celle-ci est utilisée pour prendre en charge le service de téléphonie sur IP (ToIP).

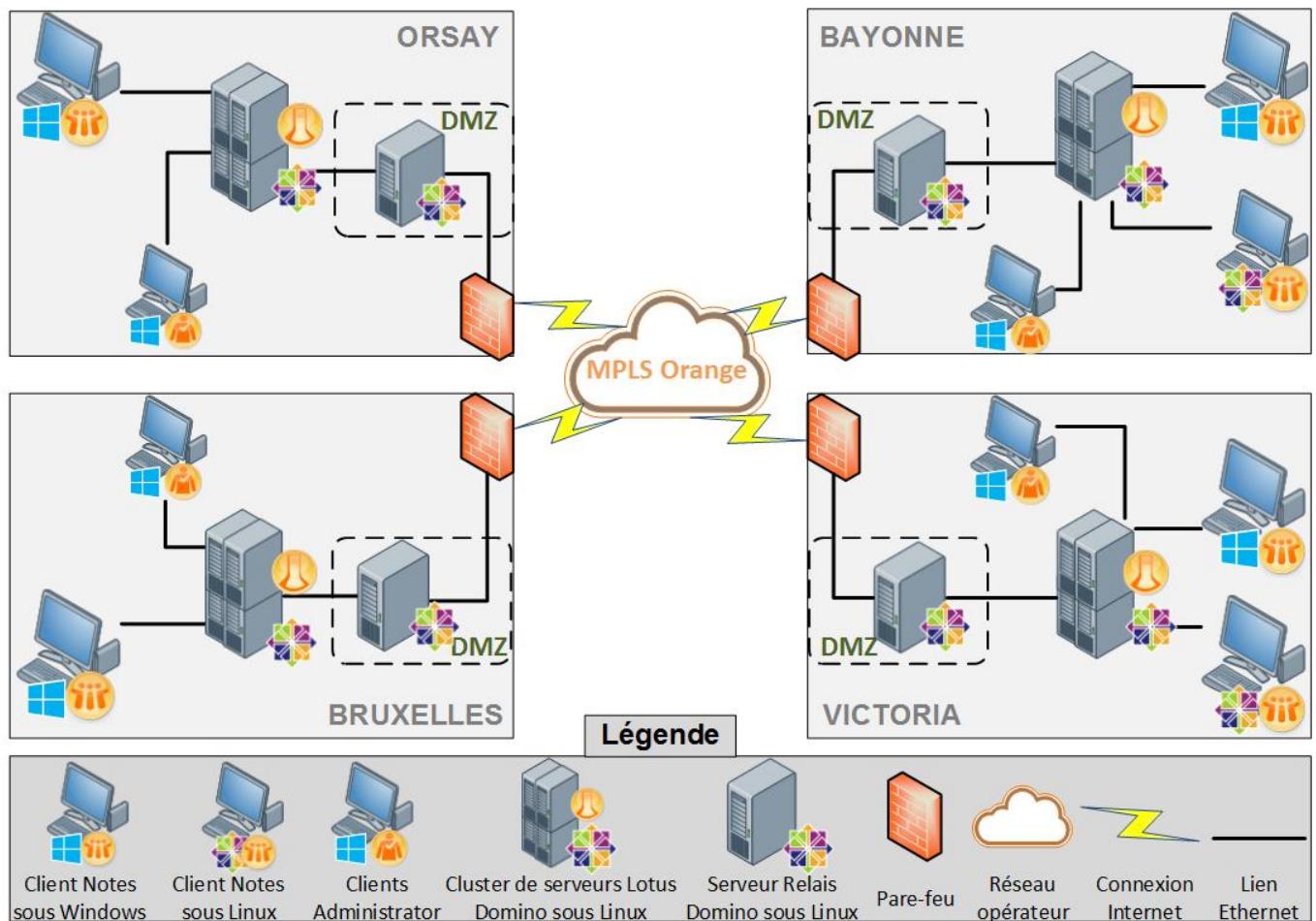
ANNEXE 1 : TOPOLOGIE LOGIQUE DE LOTUS DOMINO 8.5

Auteur : Benoit CALLABET



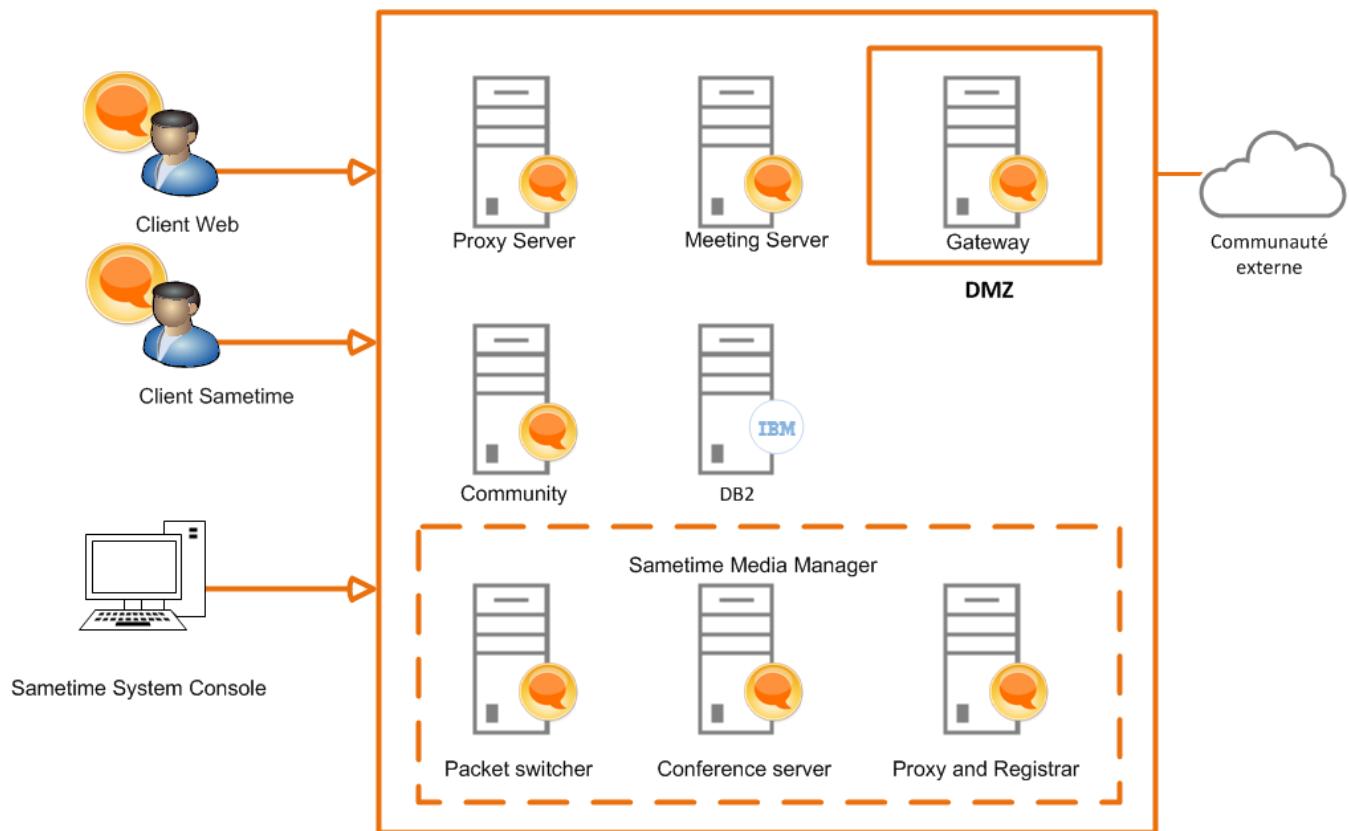
ANNEXE 2 : TOPOLOGIE PHYSIQUE DE LOTUS DOMINO 8.5

Auteur : Sothirak PHE



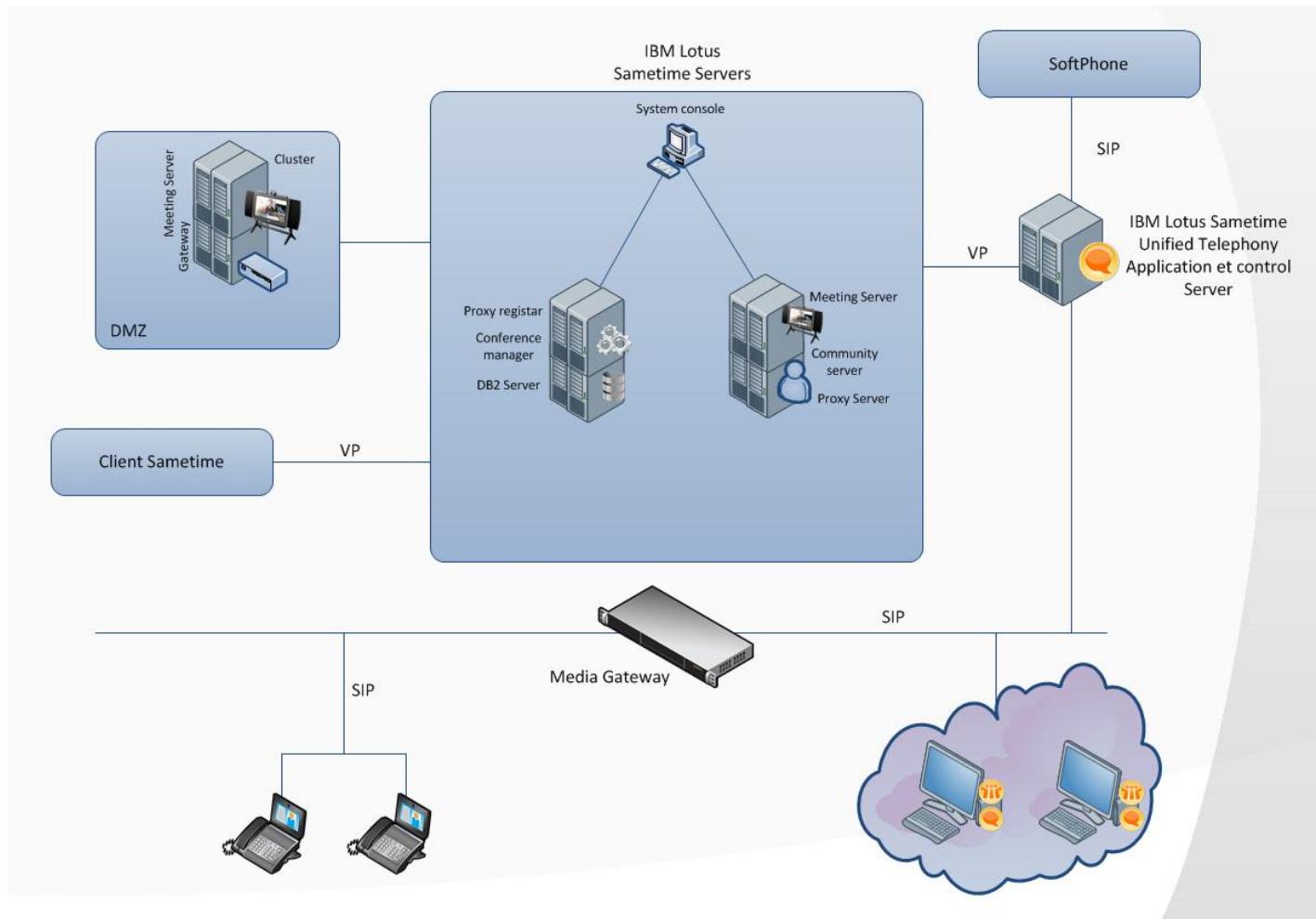
ANNEXE 3 : TOPOLOGIE LOGIQUE DE LOTUS SAMETIME 8.5

Auteur : Chris CESBRON



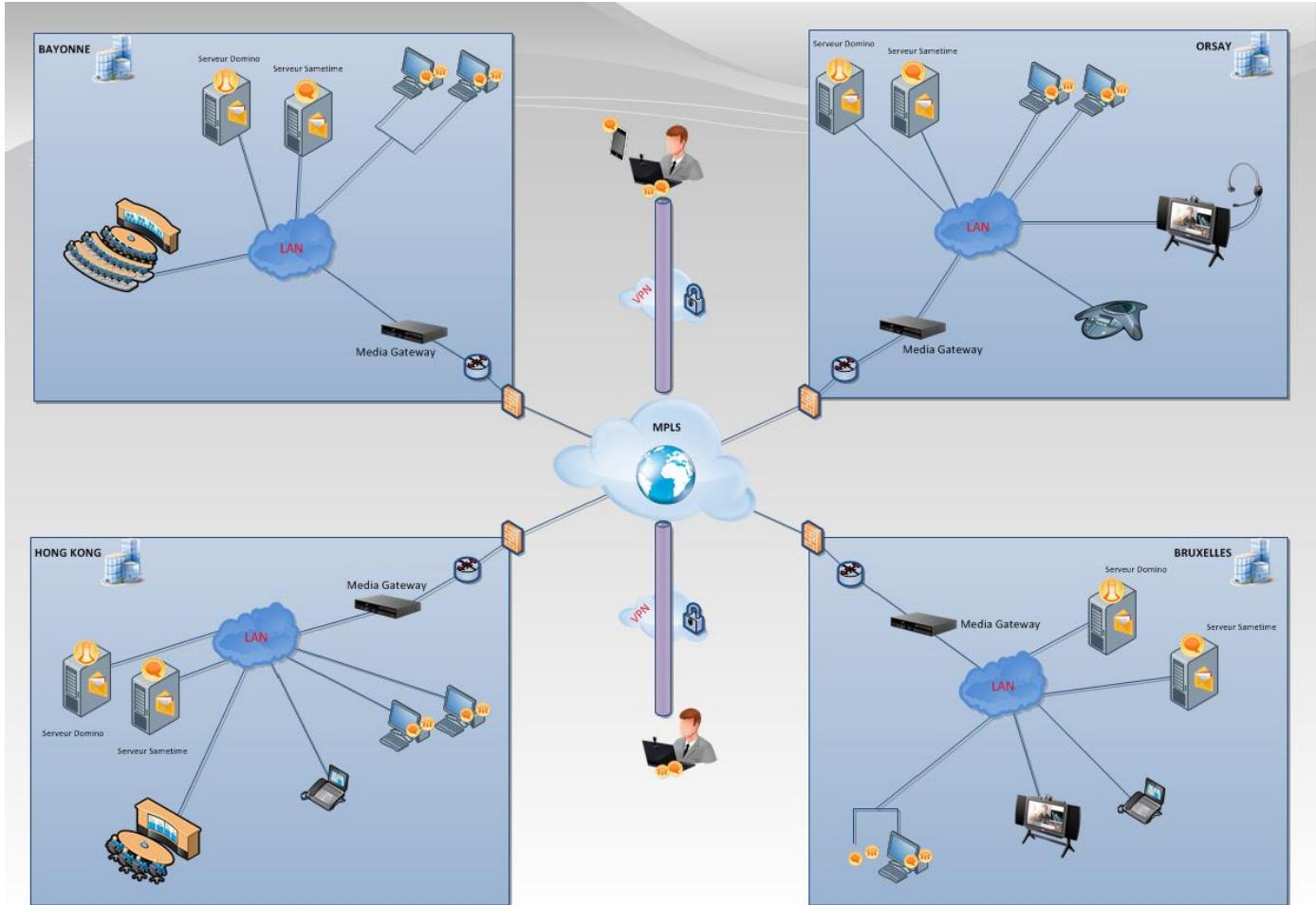
ANNEXE 4 : TOPOLOGIE PHYSIQUE DE LOTUS SAMETIME 8.5

Auteur : Chris CESBRON



ANNEXE 5 : COMPLEMENT DE L'ARCHITECTURE TELEPHONIQUE DE LOTUS SAMETIME 8.5

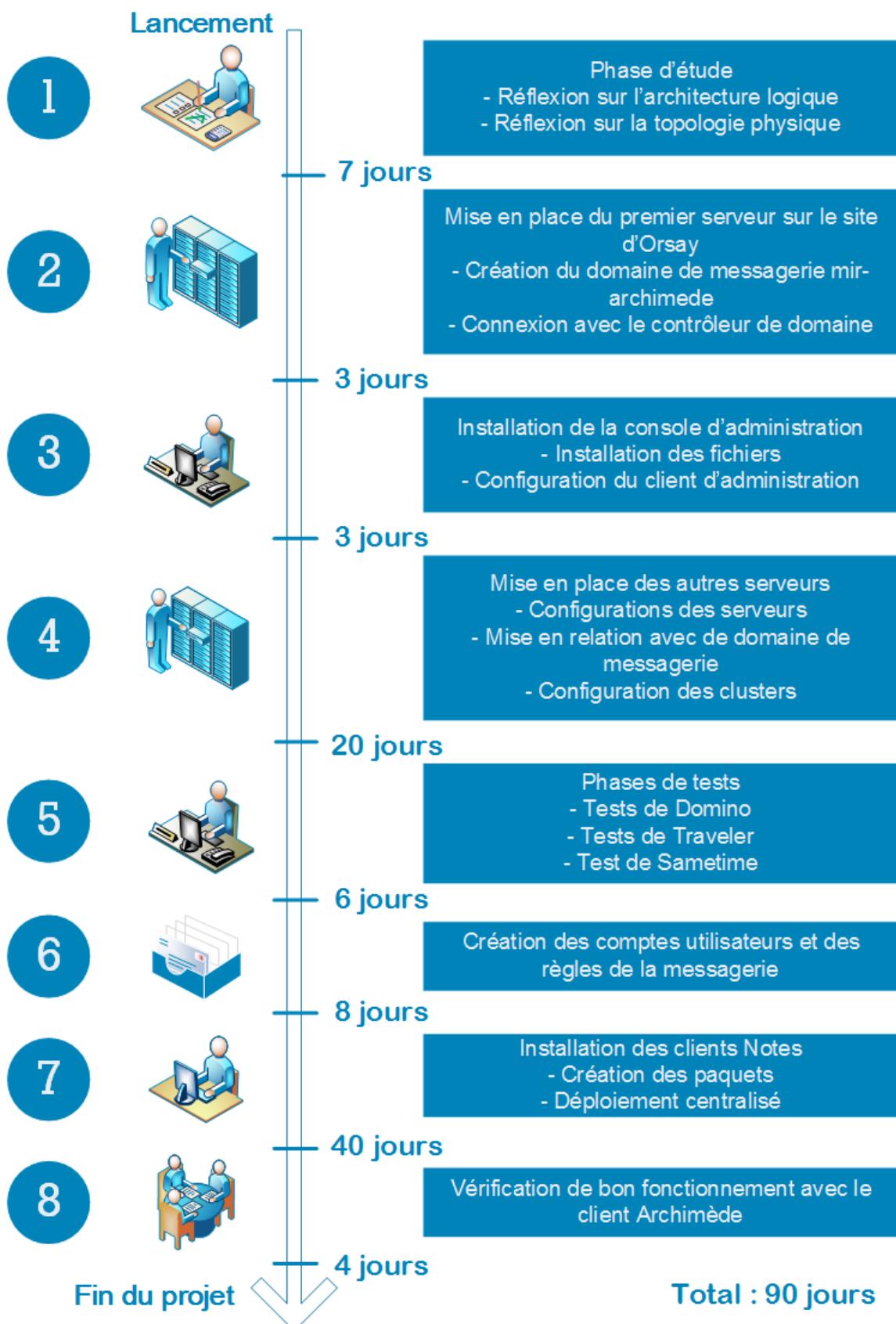
Auteur : Chris CESBRON



Les entreprises ont besoin d'échanger des informations rapidement pour améliorer et accélérer la prise de décision. L'une des clés de l'amélioration de la productivité et de la réactivité de ces quatres entités consistera à distribuer les outils de communication et de collaboration nécessaires pour faire avancer ces décisions. En intégrant la téléphonie à la plateforme globale de communication de la société, il est possible d'accélérer la prise de décision et le traitement de l'activité. L'intégration de la téléphonie permet les interactions entre deux personnes et plus. La mise en place de ce matériel sera connecté sur les serveurs de messageries instantanées Lotus Sametime étant intéropérables avec toutes les marques de téléphones qui utilisent le protocole SIP.

ANNEXE 6 : PLANNING DU PROJET DE LOTUS DOMINO 8.5 ET DE LOTUS SAMETIME 8.5

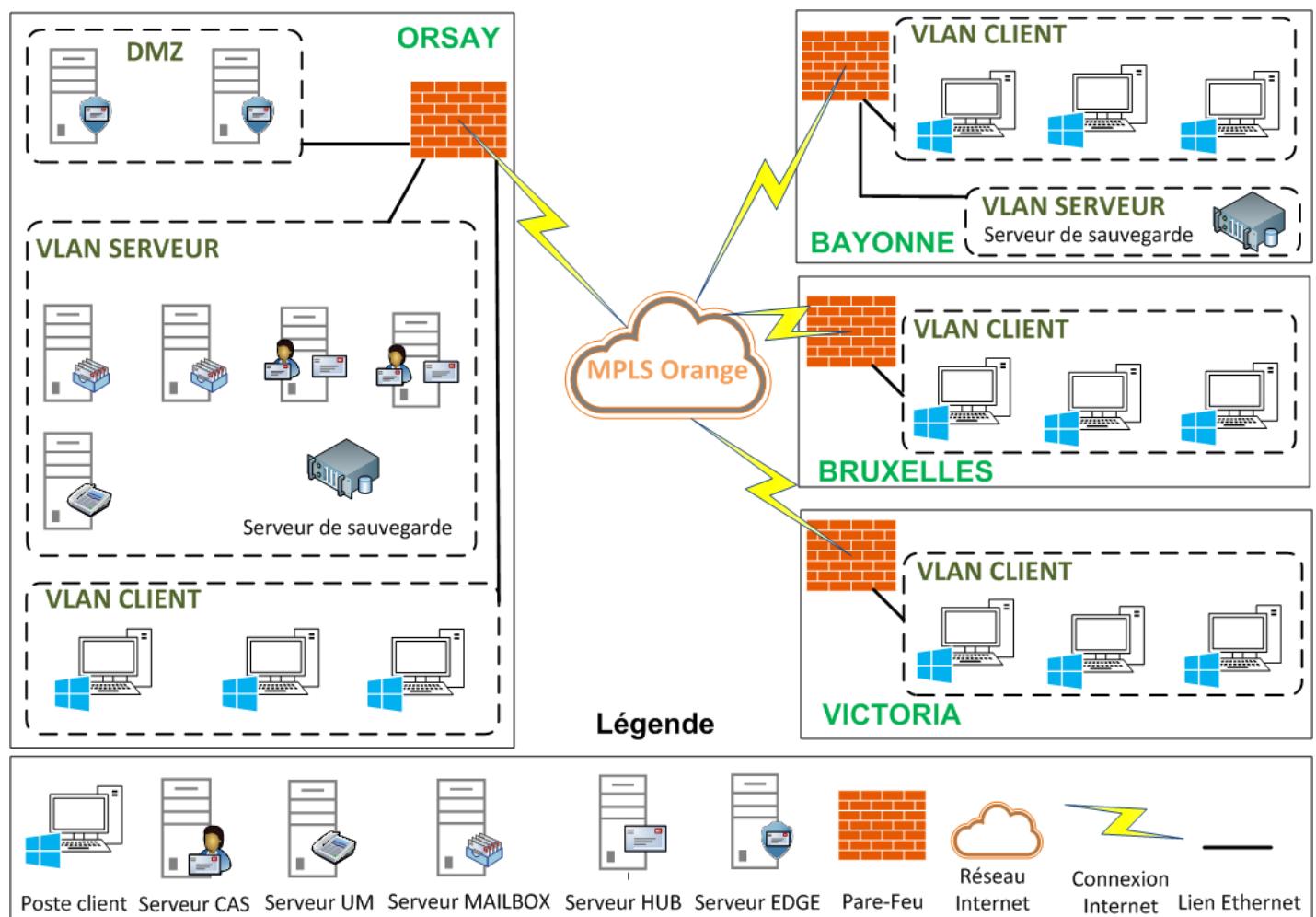
Auteur : Sothirak PHE



ANNEXE 7 : TOPOLOGIE LOGIQUE D'EXCHANGE

2010

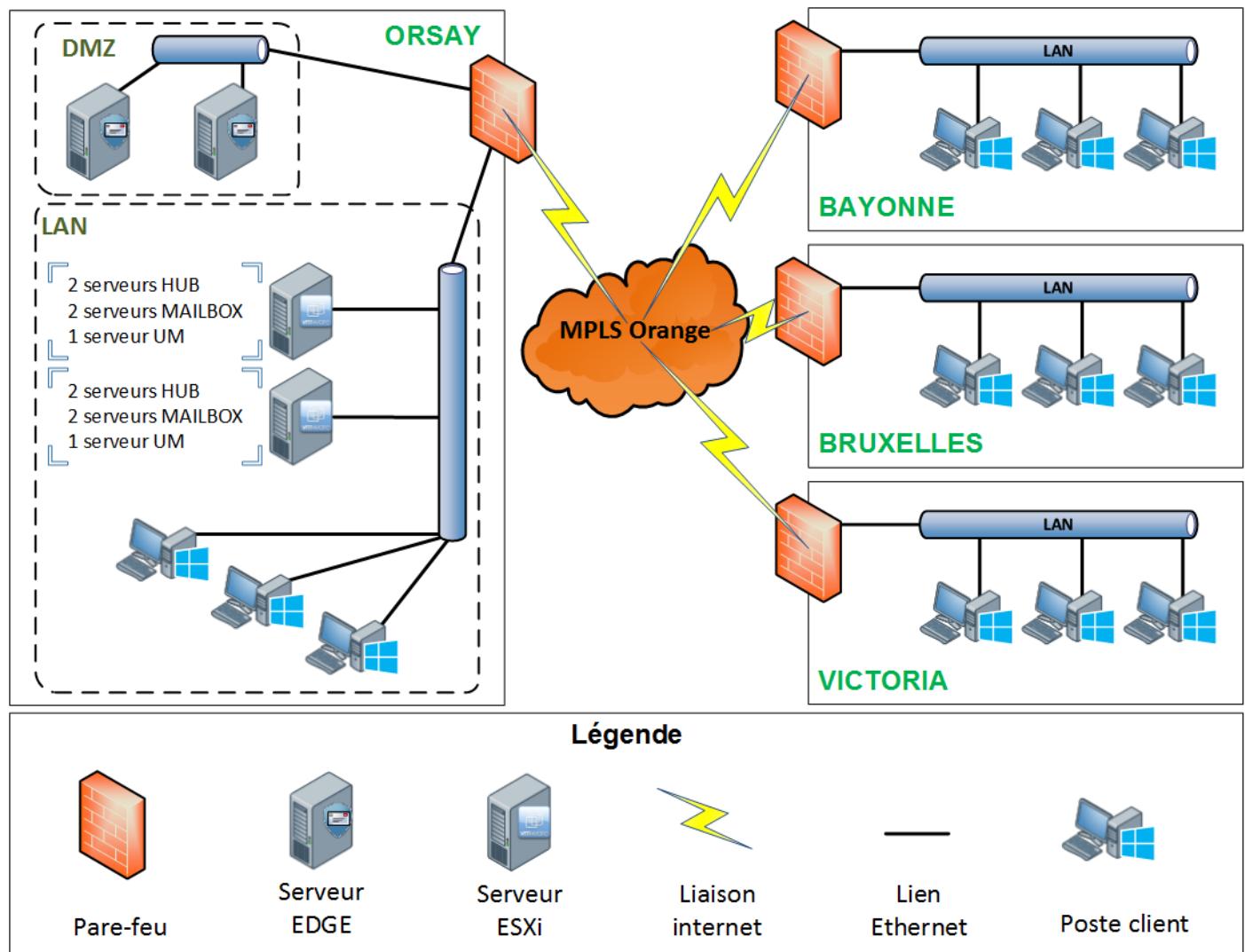
Auteur : Jérôme GOUPIL



ANNEXE 8 : TOPOLOGIE PHYSIQUE D'EXCHANGE

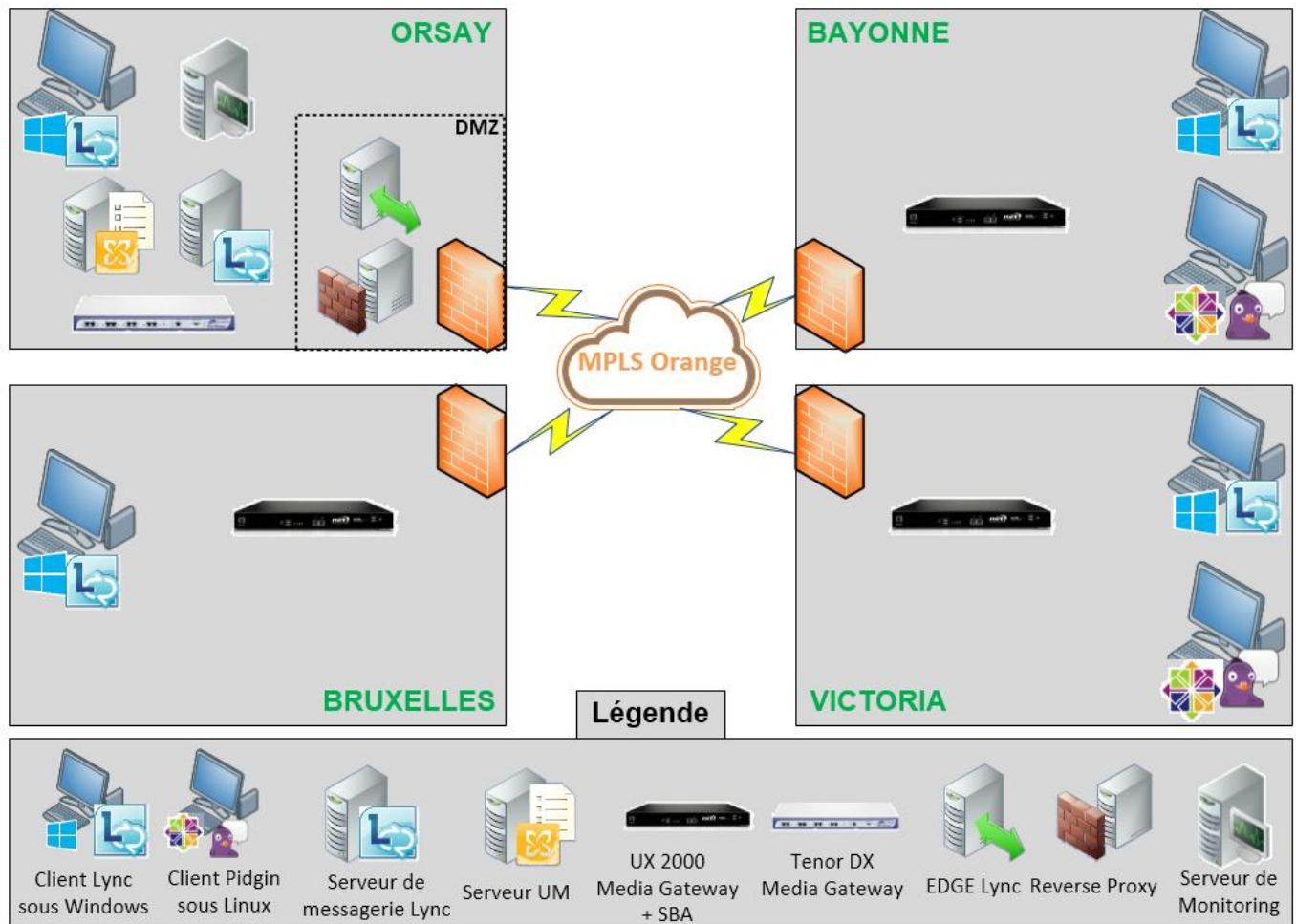
2010

Auteur : Jérôme GOUPIL



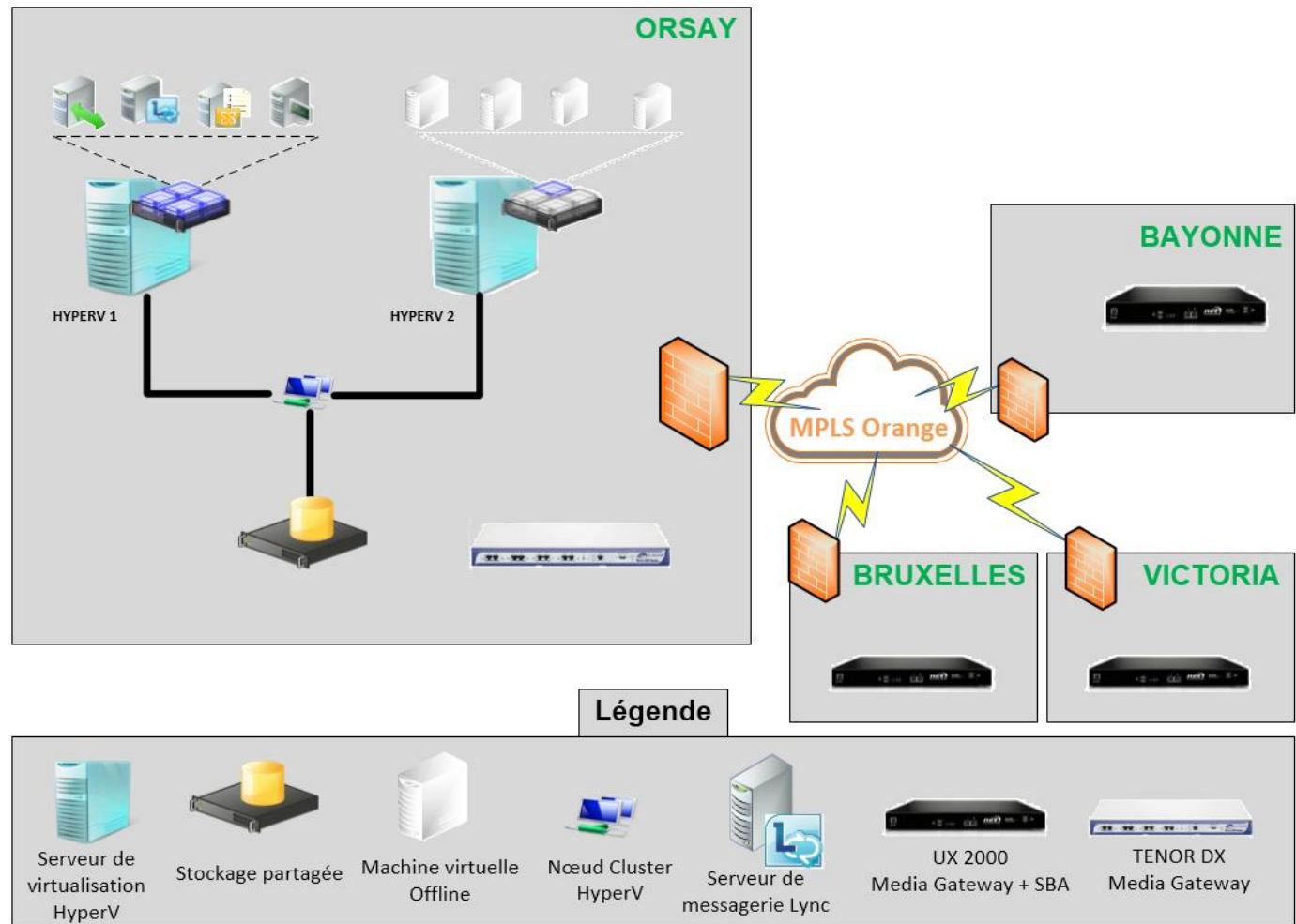
ANNEXE 9 : TOPOLOGIE LOGIQUE DE LYNC 2010

Auteur : Nicolas BROISIN



ANNEXE 10 : TOPOLOGIE PHYSIQUE DE LYNC 2010

Auteur : Nicolas BROISIN



ANNEXE 11 : PLANNING DU PROJET D'EXCHANGE 2010 ET DE LYNC 2010

Auteur : Nicolas DOSTERT



ANNEXE 12 : BESOINS MATERIELS D'EXCHANGE ET DE LYNC 2010

Auteur : Jérôme GOUPIL

1) Serveurs

Serveur utilisé pour la virtualisation des rôles de messagerie :

DELL PowerEdge R520



Caractéristiques	Prix
Processeur Xeon 8 cœurs Mémoire vive : 32 Go Disque dur : 2 x 146 Go	3 700€

2) Support de stockage pour les machines virtuelles :

Pour le stockage des machines virtuelles, nous utiliserons un serveur de stockage de type

Dell PowerVault MD3200i



Caractéristiques	Prix
4 disques durs de 2 To en raid 5	7 070€

3) Robots de sauvegarde à disposer sur le site d'Orsay et sur Bayonne (PRA) :

Pour la sauvegarde sur bande, nous avons sélectionné le robot de sauvegarde suivant :

Dell PowerVault TL2000



Caractéristiques	Prix
Magasin de stockage de 48 emplacements Compatible avec la plupart des bandes sur le marché.	11 180€

Les sauvegardes des machines virtuelles (Exchange & Lync) et des différentes bases de données seront effectuées de la manière suivante :

- ✚ Une sauvegarde complète chaque dimanche à 2h du matin,
- ✚ Une sauvegarde journalière incrémentielle la nuit.

ANNEXE 13 : COMPLEMENTS DES COUTS D'EXCHANGE 2010

Auteur : Jérôme GOUPIL

Licences Exchange nécessaires - côté serveur :

Une licence par serveur Exchange est nécessaire. Concrètement, si l'entreprise dispose de quatre serveurs quatre licences seront nécessaires. Il existe deux éditions serveur d'Exchange :

La version Standard et l'Entreprise, la différence majeure entre ces deux éditions réside dans sa capacité à gérer des bases de données (L'édition peut gérer jusqu'à cinq bases de données alors que l'édition entreprise peut gérer jusqu'à 100 bases de données).

Nous sélectionnons la version Standard pour le client Archimède.

Licences Exchange nécessaires - côté client :

Les licences côté client sont nommées licence « CAL ».

Comme pour les serveurs il en existe deux types :

La Standard et l'entreprise. Si vous souhaitez accéder aux fonctions standards d'Exchange, il vous faudra une licence CAL standard. Si vous souhaitez accéder aux fonctions avancées d'Exchange, il vous faudra une CAL standard ainsi qu'une CAL entreprise. Ces CAL n'ont rien à voir avec l'édition de votre architecture Exchange puisque la seule différence sur ces éditions est le nombre de bases gérées.

La Version CAL entreprise sera sélectionnée pour le client Archimède. 820 seront nécessaires, mais nous en prévoyons 100 de plus afin de prévoir une augmentation de l'effectif du client Archimède.

(Ici nous n'incluront pas le coût d'achat d'un client de messagerie car Outlook est intégré dans le pack Microsoft Office).

ANNEXE 14 : COMPLEMENT DES COUTS DE LYNC

2010

Auteur : Nicolas BROISIN

Voici un tableau qui récapitule les licences serveurs nécessaires pour le projet :

Rôle serveur	Coût Licence Lync	Version Windows	Coût
Lync Frontend Standard	700€	2008 SP2 standard	750 €
Lync Monitoring	Compris dans licence	2008 SP2 standard	750 €
Lync Edge Server	Frontend	Compris dans licence	750 €
Exchange 2010 UM	Frontend	2008 SP2 standard	Compris dans les coûts Exchange

Il faut ajouter à cela 2 Licences Windows 2008 Entreprise pour les 2 serveurs de virtualisation HyperV afin qu'ils puissent avoir la possibilité de faire un cluster d'HyperV : $3000\text{€} * 2 = 6\,000\text{€}$

NET Tenor DX gateway



Prix: 1500€

Nombre: 1

Coût: 1500€

NET UX 2000 gateway



Prix Unitaire : 3000€

Nombre: 3

Coût: 9 000€

Voici un tableau qui récapitule les licences client Lync 2010 nécessaires pour votre projet :

Fonctionnalités	CAL Utilisateur Standard	CAL Utilisateur Enterprise	CAL Utilisateur Plus
Messagerie instantanée et présence	X	X	X
Audio Vidéo et Web conférencing		X	X
Téléphonie d'entreprise			X
Coût	35€	+ 100€	+ 100€

Nous utiliserons une CAL Entreprise pour satisfaire les besoins actuelles et lors de l'évolution vers de la téléphonie d'entreprise il faudra demander une CAL Utilisateur « Plus » qui demandera 100€ en plus pour chaque utilisateur.



La licence client lourd de Lync 2010 est de 30€.

Le client lourd Pidgin ne nécessite pas de licence car provenant de la communauté open source Linux.

ANNEXE 15 : DESCRIPTION DES ROLES DE LYNC

Auteur : Nicolas BROISIN

Rôles en zone Interne

Ci-dessous le détail des services gérés par un serveur Lync Frontend standard :

Le rôle Frontal « Front End »

Ce serveur permet d'initier les communications SIP (session initiation protocole) entre les clients et les serveurs. Ce serveur frontal héberge les serveurs de messagerie instantanée, de présence, de téléphonie, de conférence et toutes les opérations essentielles de services aux utilisateurs.

Le rôle « Lync Web App »

Pour les utilisateurs ne possédant pas le client Lync 2010 sur leur poste de travail ou pour permettre l'accès aux services Lync depuis un ordinateur public par exemple, le rôle LWA permettra de se connecter grâce avec un simple navigateur Web (Microsoft ou autre). Il sera alors possible de réaliser des conversations instantanées mais aussi de profiter de nouvelles fonctionnalités de pont de conférence audio ou encore d'utiliser la fonctionnalité de partage du bureau.

Le rôle « Audio/vidéo Conferencing »

Le serveur « audio/vidéo Conferencing » est dédié au MCU (Multi Control Unit) pour les conférences Audio/Vidéo dans un scenario de haute disponibilité. Ce serveur permet aux utilisateurs de partager des flux audio et vidéo.

Le rôle « Web Conferencing »

Le serveur « Web Conferencing » est dédié au MCU (Multi Control Unit) pour les conférences Web. Ce serveur permet les conférences sur site.

Le rôle « Composants Web »

Il s'agit d'un serveur IIS, dédié aux données de conférences WEB. Ce serveur permet aux utilisateurs d'effectuer d'accéder principalement à des présentations de réunions et autres contenus de conférences Web ;

Rôle Médiation

Le serveur de médiation est un composant nécessaire pour l'implémentation de la téléphonie d'Entreprise et la solution de conférence Audio avec l'extérieur (PSTN).

Le serveur de médiation convertit la signalisation, et dans certains cas spécifiques les flux Audio entre l'infrastructure Lync et le monde externe à l'entreprise. Dans notre cas le rôle de médiation sera intégré à notre voice Gateway.

Rôle de monitoring

Ce serveur surveille la QoE (qualité d'expérience) pour la voix et les médias. Il génère des rapports complets ainsi que les historiques des analyses. C'est un élément clé dans l'architecture Lync car cet outil permettra de superviser le bon fonctionnement des échanges entre les collaborateurs et d'intervenir éventuellement sur les composants réseaux en cas de dysfonctionnements mis en évidence dans les rapports.

Ce serveur inclut également la possibilité d'avoir des « statistiques » d'utilisation sur le nombre de conversations instantanées, le nombre de conférences audio et/ou vidéo effectuées ou encore le nombre d'appels émis entre les collaborateurs ou avec l'extérieur dans le cas où Lync serait couplé avec la téléphonie de l'entreprise.

Rôles en zone Externe

Afin de permettre les accès externes aux services Lync, un serveur Lync Edge doit être déployé dans une DMZ. Les serveurs Lync Edge n'appartiennent pas à une forêt Active Directory mais sont installés dans un groupe de travail (Workgroup).

La configuration recommandée dans le cas de déploiements comme le groupe est de déployer un seul serveur Edge consolidé.

Il est également nécessaire de déployer une machine avec la fonction http Reverse Proxy pour la publication de services clients. Dans notre cas nous déployerons ce rôle sur notre Edge.

Ci-dessous le détail des services gérés par un serveur Lync Edge :

Le rôle « Access Edge »

Ce serveur gère les accès distants des utilisateurs, la fédération avec une entreprise possédant également OCS 2007 ou Lync 2010 ainsi que la connexion aux messageries instantanées publiques (AOL, Yahoo et MSN).

Le rôle « Audio/vidéo Conferencing Edge »

Ce serveur permet le transport du trafic des conférences Audio/Vidéo à travers les réseaux de périmètre, pour les utilisateurs externes. Il prend également en charge les services de conférences audio et/ou vidéo, le partage d'applications et les communications peer to peer avec les utilisateurs externes.

Le rôle « Web Conferencing Edge »

Le rôle de ce serveur est de transporter le trafic des conférences WEB organisées dans l'entreprise à travers les réseaux de périmètre pour les utilisateurs externes, anonymes ou fédérés.

Ci-dessous le détail des services gérés par le serveur HTTP Reverse Proxy :

Le rôle « HTTP Reverse Proxy »

Le rôle de ce serveur est de mettre à disposition des utilisateurs externes les fonctionnalités suivantes :

- Téléchargement du carnet d'adresses pour Le client Lync 2010
- Expansion des contacts pour les groupes de distribution
- Téléchargement de contenu pour les conférences (fichiers ppt, Excel, ..)
- Mise à jour des périphériques (téléphone IP) et des clients.
- point à point avec les utilisateurs externes.