

Luc Soriano

Epitech



MSC PRO : Architecte système réseau et sécurité



alinea

RAPPORT DE L'ACTIVITE EN ENTREPRISE

Administration Systèmes & Réseaux,
développement du service informatique et
support

Luc Soriano

Alinéa

2290 Route de Gemenos
13785 Aubagne
Bouche du Rhone

Responsable en Entreprise : Jean-Charles Verrazi / Stéphane Jeannot

Promotion 2019 – 2021

Remerciements

Mes remerciements les plus sincères à toutes les personnes ayant permis, de près ou de loin, le bon déroulement de ces années d'alternance.

Remerciements à l'équipe enseignante :

À l'ensemble des responsables pédagogiques pour leur disponibilité, la qualité des supports de projets et les nombreuses ressources mises à notre disposition au cours de ces deux années de formation.

Remerciements à mes collègues

À l'ensemble d'Alinéa pour son accueil et l'ambiance d'entraide au sein de l'entreprise :

- Stéphane Jeannot, mon tuteur partie *Système Réseaux et sécurité* pour sa patience, sa bienveillance et son aide au quotidien.
- Jean-Charles Verazzi, mon tuteur pour la partie *Devops* pour son soutien technique.
- À l'équipe IT, pour ces 2 ans.
- Et plus largement, à toutes les équipes d'Alinéa.

Sommaire

Table des matières

Introduction.....	5
Présentation de l'Entreprise.....	6
En bref.....	6
Les équipes.....	6
Mon Organisation	8
Organisation de L'IT	8
Gestion de projet et méthodologie.....	8
Support utilisateurs.....	9
Des missions diverses.....	9
Mes Missions	10
Gestion du parc informatique	10
Gestion des équipements internes	10
Politique de sécurité des mots de passes	12
Mot de passe complexe	12
Changement régulier	13
Déploiement Wiki entreprise.....	14
Le projet	14
L'étude du projet.....	14
La réalisation du projet	15
Rajout d'une base de données	17
Gestion du parc Mobile d'Alinéa.....	19
L'outil	19
La gestion du MDM	19
Ma mission dans SOTI	20
La partie application.....	22
La partie Kiosque.....	23
La méthodologie	23
VOIP.....	24
Le sujet	24
L'outil	24
La Quality of Service (QoS)	25
Les Mailbox.....	26
Déménagement du datacenter.....	27
Contexte.....	27
Dérouler du déménagement.....	27
Scénario du déménagement	28
Services attendus	29
Ma partie du déménagement.	29

Les problèmes rencontrés	29
Conclusion	30
Mise en place VPN pour MAC	30
VMWare et Active Directory	31
Le Sujet	31
Les outils.....	32
Mes missions.....	33
Conclusion	33
Bilan	34
Conclusion	35
Glossaire	36
Annexes	38

Introduction

Ce document constitue le rapport de mes deux années d'alternance chez Alinéa.

Durant mes 2 années d'alternance, l'équipe IT d'Alinéa a été confrontée à un changement majeur. En effet, à cause de la crise sanitaire, 90% de l'infrastructure physique d'Alinéa (comportant l'ensemble des serveurs physiques) a dû être exportée pour devenir un cloud privé, hébergé par Jaguar Network.

Avec ce choix de la direction et les différentes équipes qui composent l'IT, plusieurs problèmes concernant la gestion du parc ainsi que son évolution ont été soulevés. Beaucoup d'éléments étaient donc à modifier, améliorer ou à changer.

Mes missions cette année ont principalement concerné la gestion du parc informatique d'Alinéa qui comprend de multiples tâches, le déménagement de la salle informatique, la gestion du déploiement d'application mobile ainsi que la création et le support de plusieurs nouveaux service pour l'entreprise.

Dans ce rapport, je m'attarderai principalement sur les tâches listées ci-dessus, cependant cette liste n'est pas exhaustive car durant les 2 ans j'ai effectué de nombreuses autres tâches bien plus courtes comme du support, ou de l'installation de matériel, etc. ...

Je présenterai dans un premier temps, le contexte dans lequel j'ai évolué, avec un rappel sur l'entreprise, l'organisation d'équipe et de l'IT, l'évolution de l'entreprise durant ces deux années et mon positionnement dans ce contexte.

Je développerai mes missions sur ces années, les grands axes de travail pour le développement de l'infrastructure ainsi que des multiples changements qu'a subi Alinéa.

Je terminerai par un bilan, en analysant les conditions dans lesquelles mes projets ont été menés, l'état des lieux « avant – après » et l'impact de mes deux années sur l'entreprise.

Présentation de l'Entreprise



Alinéa est une marque et une entreprise commerciale française de décoration et d'ameublement appartenant aux actionnaires de l'association familiale Mulliez (AFM).

Elle dispose de 9 grands magasins dans toute la France.

En bref

L'enseigne spécialisée en ameublement et décoration est créée le 29 juin 1988 à Avignon. Avec un magasin de 1989 à 1996, Alinéa démarre son expansion à partir de 1997 avec l'ouverture d'un deuxième magasin à Montpellier. En 2015, Alinéa, avec 26 magasins, atteint un chiffre d'affaires de 520 millions d'euros.

Le 16 mai 2020, son directeur Alexis Mulliez annonce avoir déclaré l'état de cessation de paiement de l'entreprise. L'enseigne est donc placée en redressement judiciaire par le tribunal de commerce de Marseille après n'avoir réussi à sauver que 15 % de son chiffre d'affaires au cours des deux mois de confinement.

Grâce à une nouvelle loi intervenue en contexte de Covid-19, des dirigeants ayant déposé le bilan d'une entreprise peuvent de nouveau diriger cette entreprise. L'offre de la famille Mulliez prévoit toutefois la fermeture de grands nombres de magasins pour n'en conserver que 9, essentiellement dans le Sud de la France. Au total, seuls 900 des 1974 employés sont gardés.

Concernant son Business Model, Alinéa fonctionne comme une chaîne classique de magasin d'ameublement. Elle développe cependant de plus en plus le E-commerce pour se positionner en avant du marché et répondre à la demande client.

Les équipes d'Alinéa s'organisent autour de plusieurs pôles détaillés ci-après.

Les équipes

Marque et style Chargée des études de marché et de la concurrence, de l'appui des commerciaux et de la communication de l'entreprise. L'équipe Marketing se charge entre autres de la réalisation de supports visuels de l'entreprise, d'étude de cas clients, de la génération de pistes commerciales par le biais du site web des catalogues ou par des campagnes de publicité.

L'équipe Produit Chargée du contrôle de gestion et d'approvisionnement ainsi que du packaging et du contrôle qualité, leur travail est d'assurer la logistique d'approvisionnement des magasins et du siège. Ils sont également chargés de démarcher les transporteurs, d'obtenir les VISAS de transport, de s'occuper du

contrôle de la qualité de tous les types de pièces venant de l'étranger afin de s'assurer de la conformité avec les normes européennes.

Commerce et exploitation regroupe l'ensemble des directeurs commerciaux de l'entreprise, ainsi que le service client. Leur rôle est de définir la stratégie commerciale à adopter en magasin ou en ligne avec le E-commerce.

Le support Applicatif Chargé de la communication entre les utilisateurs et les développeurs concernant l'utilisation des outils informatique d'Alinéa. Cette équipe gère désormais les applications d'Alinéa sous tous leurs aspects. Ce sont ses membres qui ont repris la gestion de l'infrastructure d'hébergement, qui assurent la gestion, le support et les évolutions des applications.

It ou DSI en charge de la gestion des ressources techniques internes (poste de travail, téléphones, internet, alarme, salle serveur...) et de la récupération de « données » sur l'entreprise pour fournir de la visibilité au top management afin qu'il puisse prendre les meilleures décisions possibles. Il s'agit également, à terme, d'extraire les indicateurs clés de performances sur les différentes missions (ventes, livraisons, évolutions produits...) pour harmoniser l'ensemble et évaluer les points forts et les points faibles des processus métiers.

Mon Organisation

Organisation de L'IT

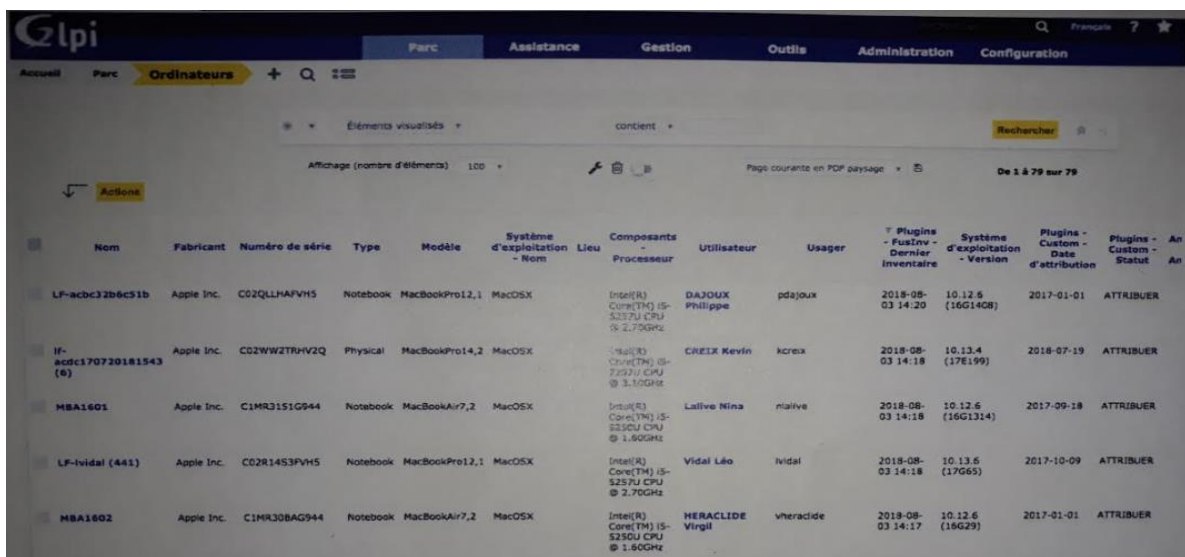
L'équipe IT est organisée sous la forme de plusieurs équipes qui s'occupent de toutes les tâches liées à l'informatique. Ainsi, on y retrouve le support admin et réseaux, le support applicatif, les techniciens physiques et les développeurs. Chaque équipe est dirigée par un responsable et M. Guillaume Lieure est le référent de l'IT. Le bureau a été pensé de façon que chaque équipe puisse profiter des compétences techniques de chacun.

Dès mon arrivée, j'ai intégré l'équipe de support administrateur système et réseaux, mon référent était alors Stéphane Jeannot.

Gestion de projet et méthodologie

Nous utilisons le logiciel de managements de projet "GLPI" pour organiser et répartir les tâches au sein de l'équipe.

GLPI aide les entreprises à gérer leurs systèmes d'information, il s'installe sur une machine type debian avec une image ISO spécifique. Une fois installée, toute la configuration s'effectue au moyen d'un navigateur web.



	Nom	Fabricant	Numéro de série	Type	Modèle	Système d'exploitation - Nom	Lieu	Composants - Processeur	Utilisateur	Usager	Plugins - Fusion - Dernier inventaire	Système d'exploitation - Version	Plugins - Custom - Date d'attribution	Plugins - Custom - Statut	An
	LP-acbc32b6c51b	Apple Inc.	C02QLHAFVH5	Notebook	MacBookPro12,1	MacOSX		Intel(R) Core(TM) i5-3230U CPU @ 2.70GHz	DAJOUX Philippe	pdajoux	2018-08-03 14:20	10.12.6 (16G1408)	2017-01-01	ATTRIBUER	
	IF-acdc170720181543 (6)	Apple Inc.	C02WW2TRHV2Q	Physical	MacBookPro14,2	MacOSX		Intel(R) Core(TM) i5-7267U CPU @ 3.10GHz	CREIX Kevin	kcreix	2018-08-03 14:18	10.13.4 (17E199)	2018-07-19	ATTRIBUER	
	MBA1601	Apple Inc.	C1MR3151G944	Notebook	MacBookAir7,2	MacOSX		Intel(R) Core(TM) i5-5250U CPU @ 1.60GHz	Lalive Nina	nlalive	2018-08-03 14:18	10.12.6 (16G1314)	2017-09-18	ATTRIBUER	
	LP-ividal (441)	Apple Inc.	C02R1453PVH5	Notebook	MacBookPro12,1	MacOSX		Intel(R) Core(TM) i5-5250U CPU @ 2.70GHz	Vidal Léo	lvidal	2018-08-03 14:18	10.13.6 (17G65)	2017-10-09	ATTRIBUER	
	MBA1602	Apple Inc.	C1MR308AG944	Notebook	MacBookAir7,2	MacOSX		Intel(R) Core(TM) i5-5250U CPU @ 1.60GHz	HERACLIDE Virgil	vheraclide	2018-08-03 14:17	10.12.6 (16G129)	2017-01-01	ATTRIBUER	

L'onglet **parc** donne accès à toutes les informations concernant le matériel réparti comme sur l'image (ordinateurs, moniteurs, numéros de série, modèles, utilisateurs, versions des systèmes d'exploitation...).

L'onglet **assistance** est très utilisé par les utilisateurs d'Alinéa car il s'agit de l'outil principal de gestion de ticket de l'entreprise. Il nous permet également de classer les

problèmes et d'obtenir des logs détaillés des différents problèmes rencontrés au cours de l'année.

L'onglet **gestion** concerne tout ce qui est administratif, c'est-à-dire les contrats, les budgets, les fournisseurs et les documents.

L'onglet **outils** pour les projets, notes, base de connaissances, réservations.

L'onglet **administration** pour les utilisateurs (les groupes auxquels ils appartiennent) et leurs profils selon leurs privilèges.

Enfin, l'onglet **Configuration** pour personnaliser l'interface WEB l'interface web ainsi que l'installation de plugins ou la liaison à d'autres solutions.

Support utilisateurs

Le support utilisateur est ainsi géré via GLPI. Nous recevons les tickets des utilisateurs puis nous les trions en fonction des types de demandes pour se les répartir entre les différentes personnes aptes à répondre aux demandes ou aux incidents.

Des missions diverses

Je suis entré chez Alinéa en tant qu'administrateur Système et réseaux (Alternant administrateur systèmes et réseaux). Dès lors, faisant partie d'une équipe de cette taille, avec un périmètre aussi large, mes missions ont été diverses et variées.

Voici un aperçu des différentes missions qui ont pu m'être confiées pendant cette année :

- Rédaction d'une partie des documentations.
- Participation à la reprise de la salle serveur.
- Participation à l'évolution de la salle serveur.
- Maintenance sur les différentes baies de disque.
- Gestion des **Raid** sur les baies de disque
- Participation aux maintenances de la plateforme.
- Mise en place de correctifs de sécurité.
- Participation à la mise en place des règles de sécurité sur les Pare-feu
- Mise en place de scripts d'automatisation de tâches.
- Mise en place de scripts pour faciliter le travail des utilisateurs.
- Déploiement d'application sur les téléphones de l'entreprise.
- Centralisation de la remonté des problèmes sur les téléphones
- Ajout d'un wiki d'entreprise via déploiement d'un conteneur WIKI

En réalité, plusieurs des projets sur lesquels j'ai été amené à travailler s'inscrivent dans une perspective plus globale.

Mes Missions

Gestion du parc informatique

Alinéa possède un très grand parc informatique celui-ci réparti sur 26 magasins (aujourd'hui 9) plus le siège.

Chaque utilisateur dispose d'un ordinateur portable (Mac ou PC) qu'ils peuvent déplacer à leur guise et aussi le ramener chez eux. Certaines personnes, notamment les Designers, possèdent des IMac fixes.

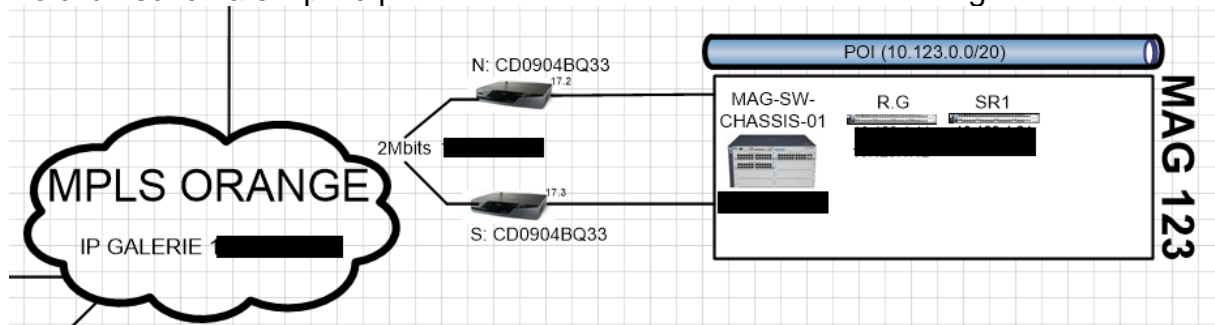
Ce choix de matériel est donc plus complexe à gérer au quotidien car il faut faire attention à ce que l'utilisateur, ayant une grande liberté, ne puisse pas ramener de malware au sein du réseau de l'entreprise surtout que ceux-ci sont généralement plus répandus sur les Systèmes Windows.

Nous nous occupons également du réseau wifi qui est composé de plusieurs bornes à travers tout le bâtiment du siège, dans la réserve ainsi que chez chaque magasin, laissant à disposition 3 réseaux wifi différents :

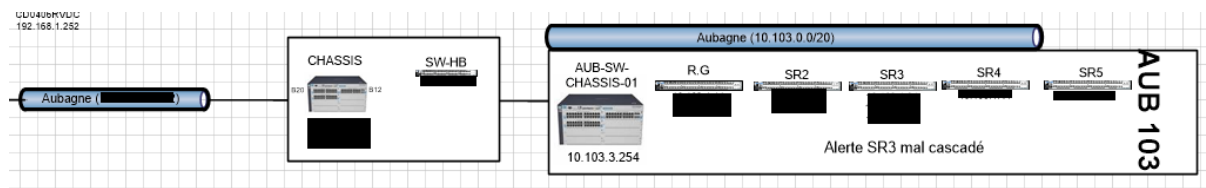
- Un réseau principal pour les utilisateurs.
- Un réseau visiteur pour les personnes présentes dans les locaux extérieurs à la société et ayant besoin d'une connexion internet.
- Un réseau qui laisse passer les configurations, notamment pour les équipements tels que les téléphones ou les **PDA**s et toutes les télévisions présentes dans chaque bureau pour la diffusion d'informations destinées aux utilisateurs.

Gestion des équipements internes

Voici un schéma simplifié présentant l'infrastructure interne d'un magasin d'alinéa :



Voici un schéma réseau simplifié de l'infrastructure de la salle 2 du siège d'Alinéa, qui avant le déménagement était notre datacenter :



Etant donné la taille du schéma de la salle siège, vous la retrouverez en Annexe.

Comme vous pouvez le voir via le schéma réseaux ci-dessus, Alinéa possède une architecture assez simple entre le siège et les magasins. Cependant, tous les serveurs d'administration, de développement, ainsi que de configuration se situent dans la salle serveur du siège et du magasin d'Aubagne. Voici une liste non exhaustive des services utilisés par Alinéa :

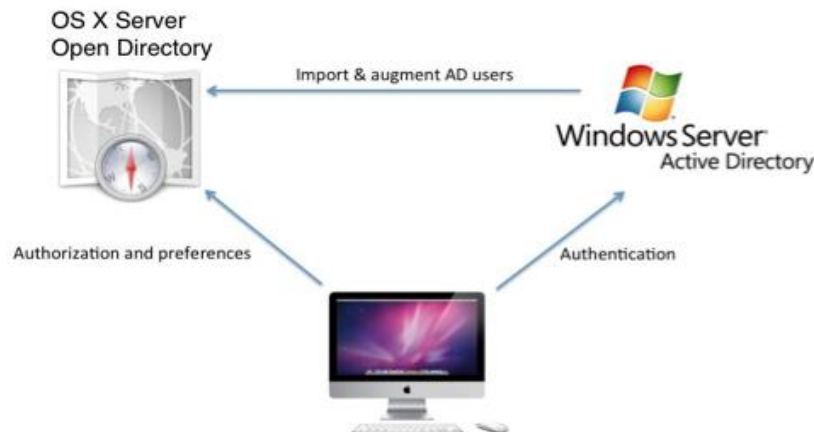
- Active directory servant à la gestion des utilisateurs
- DNS service de résolution des noms de domaine
- Spooler d'impression (gestionnaire d'impression)
- Contrôleur de domaine servant à administrer l'active directory
- DHCP : Permettant l'attribution des adresses IP aux utilisateurs
- ESx VMWare qui héberge une multitude de **VM**
- Serveur de développement : fonctionne sous une distribution linux qui permet une meilleure flexibilité aux développeurs
- MDM SOTI : qui est notre gestionnaire de configuration mobile et PDA

A mon arrivée, Alinéa possédait également un MAC serveur qui récupérait la configuration de l'active directory, et à partir de cela, il était possible de créer des profils (fichiers de configurations exécutable).

Ainsi, pour paramétrer un MacBook, il suffisait de lancer ces profils, en s'assurant qu'il ait bien un accès au Mac Server pour que la configuration remonte bien sur le MacBook.

Nous utilisons les profils suivants :

- Profil AD qui permet d'ajouter automatiquement un Mac au domaine
- Profil VPN qui permet d'accéder aux ressources internes lorsqu'un utilisateur se trouve en télétravail (hors locaux).
- Profil écran d'accueil spécifique et personnalisé qui permet aux utilisateurs de se logger.
- Profil de mise à jour centralisée pour garder à jour les Mac des utilisateurs automatiquement et sans action de leur part.



Ce service était sur le déclin, Apple ayant arrêté depuis bien longtemps le support des Macs Server, il a été retiré deux mois après mon arrivée.

Politique de sécurité des mots de passes

Mot de passe complexe

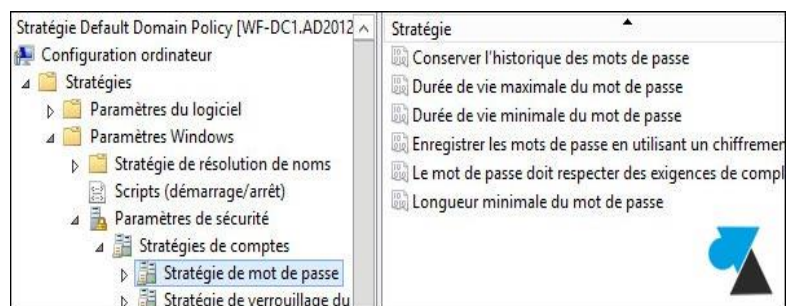
Juste avant mon arrivée, il a été décidé d'améliorer la politique des gestions de mots de passe.

Si l'utilisation d'un keypasse, qui est un coffre-fort de mot passe, est un plus, il n'en reste pas moins que la politique de gestion des mots de passe reste très mauvaise.

Il n'y avait aucun renouvellement de mots de passe, pas de longueur minimum, pas de caractères spéciaux exigés...

Je me suis chargé de la communication sur le sujet ainsi que du renouvellement de mot de passe via la GPO sur l'AD.

Tout d'abord, j'ai vu chaque utilisateur de l'entreprise pour cocher sur son profil : « l'utilisateur devra changer son mot de passe » après avoir appliqué une GPO sur l'ensemble du groupe Utilisateurs.



Il s'agissait avant tout de mettre des mots de passe sécurisés.

La première version du modèle de complexité de mot de passe a d'abord été :

- Un minimum de 8 caractères
- Une majuscule et une minuscule
- Obligation d'avoir chiffre(s) et lettre(s)
- Un caractère spécial minimum
- Conserver l'historique des mots de passe sur les 10 derniers utilisés.

Cependant, après le changement de mot de passe un problème est très vite apparu.

En effet, pour gérer la sécurité du disque dur sur certain MacBook, nous activons FileVault sur chaque MacBook de l'entreprise.

Le problème est que sur certains MacBook AZERTY, notamment les 12.1, si un caractère spécial est présent dans les mots de passe, au démarrage le clavier passait automatiquement en QWERTY. Le problème a été reconnu par Apple mais ils ne comptent pas s'en occuper étant donné le faible pourcentage que représente l'utilisation du clavier AZERTY sur leur marché.

Nous avons donc dû abandonner l'exigence du caractère spécial dans les mots de passe, pour les utilisateurs utilisant un Mac avec FileVault. En conséquence, nous avons passé notre mot de passe de 8 caractères à 12 caractères.

Changement régulier

La deuxième étape fut d'instaurer une politique de changements réguliers de mots de passe.

Via une GPO, j'ai organisé un renouvellement de mots de passe 90 jours après le dernier renouvellement.

Cependant, vu le nombre d'utilisateurs pratiquant le télétravail dans l'entreprise, il était important de les prévenir automatiquement et longtemps à l'avance, pour que nous n'ayons pas à gérer les dates de renouvellement de chaque utilisateur.

J'ai donc réalisé un script en powershell (observable en entier dans les annexes) permettant de comparer la dernière date de changement de mot de passe avec la date d'expiration du mot de passe et d'en tirer un nombre de jours avant le prochain changement.

En bref, le script va d'abord chercher les comptes qui n'ont pas de `passwordNeverExpires` et comparer le temps restant aux mots de passes par rapport à son `PasswordLastSet` :

```
#Trouve les comptes qui sont actifs et qui ont un mot de passe "PAS illimitÃ©"
$users = Get-ADUser -filter {Enabled -eq $True -and PasswordNeverExpires -eq $False -and PasswordLastSet -gt 0 } `
-Properties "Name", "EmailAddress", "msDS-UserPasswordExpiryTimeComputed" | Select-Object -Property "Name", "EmailAddress", `
@{Name = "PasswordExpiry"; Expression = {[datetime]::FromFileTime($_.msDS-UserPasswordExpiryTimeComputed)}.toLongDateString() }}
```

Ensuite, des `WarnDates` sont créés pour plusieurs jours avant la date de changement :

```
Import-Module ActiveDirectory
```

```
#CrÃ©ation des WarnDates pour les expirations de mot de passe future
$FifteenDayWarnDate = (get-date).adddays(15).ToLongDateString()
$SevenDayWarnDate = (get-date).adddays(7).ToLongDateString()
$ThreeDayWarnDate = (get-date).adddays(3).ToLongDateString()
$OneDayWarnDate = (get-date).adddays(1).ToLongDateString()
```

Et enfin l'envoi de mail :

```
43 #Envoie le mail pour chaque user en fonction des WarnDates
44 foreach ($user in $users) {
45     if ($user.PasswordExpiry -eq $FifteenDayWarnDate) {
46         $days = 15
47         $EmailBody = $BodyUser -join ' '
48         $EmailTitle = $SubjectUser, $days, "jours" -join ' '
49
50         Send-MailMessage -To $user.EmailAddress -From $MailSender -Subject $EmailTitle -SmtpServer $SMTPserver -Body $EmailBody
51     }
52 }
```

Déploiement Wiki entreprise

Le projet

Alinéa utilise plusieurs services pour gérer la documentation interne. Le principal étant des lecteurs communs où les utilisateurs peuvent échanger la documentation directement via des fichiers.

C'est une méthode assez brute et des utilisateurs peuvent se perdre dans la recherche des documents.

C'est pourquoi Alinéa possède aussi un Wiki d'entreprise. Un Wiki d'entreprise est un service qui fonctionne de la même manière que Wikipédia. Il utilise le service MediaWiki qui met à disposition une page web entièrement configurable à la main et qui permet de rechercher, créer des pages de contenu où peuvent être répertorier des procédures, des photos, et même des fichiers de l'entreprise.



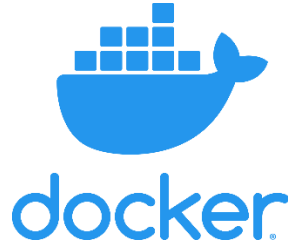
Le wiki d'Alinéa ne concerne que les utilisateurs de l'IT pour échanger et sauvegarder des procédures. C'est pourquoi, j'ai répondu à la demande de la chef de direction commerciale, et créé un autre wiki entreprise pour les utilisateurs du service commercial.

L'étude du projet

La première tâche que j'ai effectuée, a été de chiffrer le projet en heures mais également en coût.

Pour cela, j'ai voulu tout d'abord me baser sur le premier wiki qui a été installé. Cependant, je me suis vite rendu compte que l'installation datait, et que le service media-wiki n'avait pas été mis à jour. De plus, il n'y avait aucune documentation sur le sujet.

J'ai donc dû partir de zéro, et dans un souci de modernité additionné à un souhait de vouloir économiser les couts en VMs, utiliser une distribution Debian. J'ai décidé d'utiliser Docker pour déployer le service. Ainsi, si un jour, un autre Wiki est nécessaire, il ne me restera qu'à copier l'image en changeant la configuration IP du service pour pouvoir créer rapidement un nouveau Wiki.



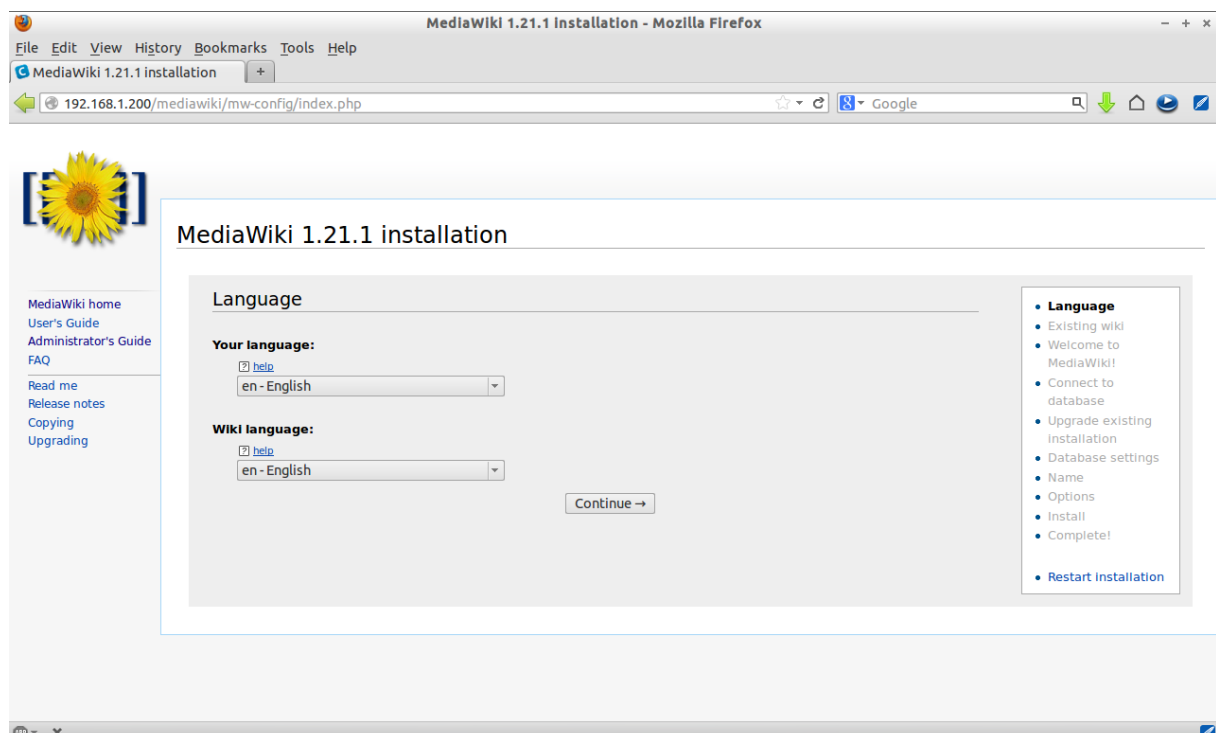
Après une présentation de mes propositions à mon responsable Jean-Charles Verazzi, le projet a été validé et j'ai pu me lancer dans sa réalisation.

La réalisation du projet

Pour commencer, j'ai installé une VM debian 10 qui hébergera le service. Je lui ai attribué une adresse IP fixe accessible sur tout le réseau de l'entreprise.

Après avoir installé le service docker j'ai pu installer l'image de Media-Wiki. Une fois installer et le port exposé dans le docker file, on arrive à ce résultat en entrant l'adresse IP du serveur suivi du port correspondant.

"docker run --name wiki-commerce -p 8080:80 --volume wiki-data:/var/www -d mediawiki:1.35"



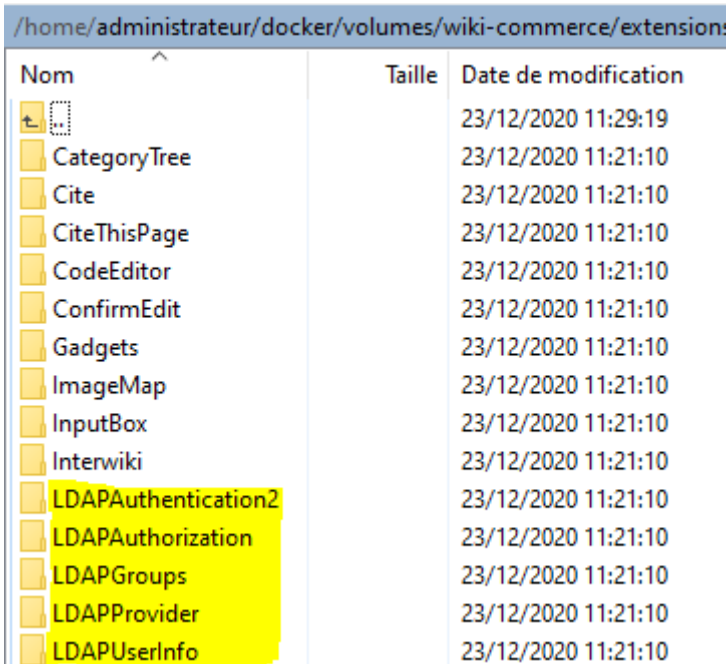
Après avoir entré nos préférences en termes de privilèges, sécurité et esthétique, le wiki est techniquement prêt.


Après avoir rendu le service accessible, il nous était indispensable de réfléchir d'un point de vue sécuritaire, quant à l'accès des ressources présentes sur le Wiki. En effet, il s'agira d'un point d'accès à de possibles ressources commerciales marketing sensibles et autres. Si une personne arrivait à se connecter au réseau de l'entreprise il pourrait accéder directement au WIKI si celui-ci n'était pas protégé par mot de passe.

Connexion avec le LDAP

Pour empêcher une personne extérieure à l'entreprise, et même plus précisément extérieure aux services concernés (commercial/marketing), d'accéder aux ressources présentes sur le Wiki, nous avons décidé avec Jean-Charles Verazzi de lier le wiki à l'Active Directory, et ainsi permettre l'accès au Wiki qu'aux personnes identifiées par l'AD.

Pour cela, nous avons rajouté de nombreux addons au service media wiki et donc au dockerfile (pour qu'une possible future installation se déroule sans problème).



Nom	Taille	Date de modification
		23/12/2020 11:29:19
CategoryTree		23/12/2020 11:21:10
Cite		23/12/2020 11:21:10
CiteThisPage		23/12/2020 11:21:10
CodeEditor		23/12/2020 11:21:10
ConfirmEdit		23/12/2020 11:21:10
Gadgets		23/12/2020 11:21:10
ImageMap		23/12/2020 11:21:10
InputBox		23/12/2020 11:21:10
Interwiki		23/12/2020 11:21:10
LDAPAuthentication2		23/12/2020 11:21:10
LDAPAuthorization		23/12/2020 11:21:10
LDAPGroups		23/12/2020 11:21:10
LDAPProvider		23/12/2020 11:21:10
LDAPUserInfo		23/12/2020 11:21:10

Ci-dessus en surligné les addons que nous avons rajoutés au service Media-Wiki.

Ses addons nous permettent via des fichiers de configuration de connecter directement Media-Wiki à notre AD.

Voici un exemple avec le fichier ldap.json :

```
{
  "alinea-1.fr": {
    "connection": {
      "server": "alinea-1.fr",
      "port": "3268",
      "user": "CN=User Process,OU=Comptes Process,OU=Utilisateurs,OU=DG,OU=Alinea,DC=ALINEA-1,DC=fr",
      "pass": "*****",
      "enctype": "clear",
      "options": {
        "LDAP_OPT_DEREF": 1
      },
      "basedn": "DC=ALINEA-1,DC=fr",
      "userbasedn": "DC=ALINEA-1,DC=fr",
      "groupbasedn": "DC=ALINEA-1,DC=fr",
      "searchattribute": "samaccountname",
      "usernameattribute": "samaccountname",
      "realnameattribute": "cn",
      "emailattribute": "mail",
      "grouprequest": "MediaWiki\\Extension\\LDAPProvider\\UserGroupsRequest\\UserMemberOf::factory",
      "presearchusernamemodifiers": [ "spacestounderscores", "lowercase" ]
    },
    "userinfo": [],
    "authorization": [],
    "groupsync": {
      "mapping": {
        "GRP_ACCES_WIKI_COMMERCE_ECRITURE": "CN=GRP_ACCES_WIKI_COMMERCE_ECRITURE,OU=ACCES,OU=WIKI-COMMERCE,OU=APPLICATIONS,DC=ALINEA-1,DC=fr",
        "GRP_ACCES_WIKI_COMMERCE_LECTURE": "CN=GRP_ACCES_WIKI_COMMERCE_LECTURE,OU=ACCES,OU=WIKI-COMMERCE,OU=APPLICATIONS,DC=ALINEA-1,DC=fr"
      }
    }
  }
}
```

Comme vous pouvez voir, il s'agit du fichier qui détient les informations pour pouvoir se connecter à l'AD et rajouter des groupes d'utilisateurs qui seront autorisés à se connecter, via leurs comptes AD, au Wiki.

Les droits peuvent être gérés de façon plus précise via un fichier de config, c'est-à-dire qui a le droit d'écriture, de lecture ou suppression d'un article etc ...

Un exemple est fourni en annexe.

Rajout d'une base de données et du reverse proxy

Puisque la connexion au service Media-Wiki utilise un système de compte, il faut donc rajouter une base donnée pour qu'elle puisse stocker les comptes et les comparer à ceux de l'AD pour autoriser ou non la connexion.

Nous avons donc installé une BDD Mariadb via Docker pour que tout le processus soit conteneuriser et ainsi facilement copiable et exportable.

```
"docker run --name commerce-database -e MYSQL_ROOT_PASSWORD=**** -v commerce-database-data:/var/lib/mysql -p 3306:3306 -d mariadb:10.5"
```

Une fois installée, la liaison se gère de la même manière qu'avec l'AD. Il faut entrer les informations de connexion dans un fichier de config présent sur le volume du conteneur docker du service Media-Wiki.

```
/home/administrateur/docker/volumes/wiki-commerce/LocalSettings.php - wiki-commerce - Editeur - WinSCP

$wgEnotifUserTalk = false; # UPO
$wgEnotifWatchlist = false; # UPO
$wgEmailAuthentication = true;

## Database settings
$wgDBtype = "mysql";
$wgDBserver = "10.13.1.113";
$wgDBname = "wiki-commerce";
$wgDBuser = "root";
$wgDBpassword = "██████";
```

Une fois la liaison effectuée, il est désormais possible de se connecter au media wiki si l'on est bien présent dans les groupes autorisés à accéder au service.

Cependant, il n'est pas livrable en l'état. Il n'est pas concevable pour des utilisateurs de rentrer une adresse IP à chaque fois qu'il est nécessaire d'accéder au WIKI.

C'est pourquoi, avec l'aide de Jean-Charles Verazzi, nous avons installé une image du service Nginx qui nous a permis de faire un reverse proxy et d'obtenir un nom propre pour notre wiki.



L'installation étant complètement terminée, voici le résultat de la commande *docker ps* :

```
root@LX-WIKI-COMMERCE-01:/home/administrateur# docker ps
```

CONTAINER ID	IMAGE	COMMAND	CREATED	STATUS	PORTS	NAMES
59c520809758	mediawiki:1.35	"docker-php-entrypoi..."	5 months ago	Up 2 months	0.0.0.0:8081->80/tcp	help-dsi
d64208c25333	mediawiki:1.35	"docker-php-entrypoi..."	5 months ago	Up 2 months	0.0.0.0:8080->80/tcp	wiki-commerce
1c89a79797bd	nginx:1.19	"/docker-entrypoint..."	5 months ago	Up 2 months	0.0.0.0:80->80/tcp, 0.0.0.0:443->443/tcp	nginx

L'outil

Une de mes missions récurrentes est la gestion du parc mobile d'Alinéa. Notre parc mobile contient près de 400 téléphones et PDA de différentes marques, et principalement Samsung, Honeywell et Zebra.

Ces téléphones sont répartis sur les différents magasins ainsi qu'au siège de l'entreprise. Etant donné les différentes situations géographiques des téléphones, il était nécessaire qu'Alinéa choisisse une solution de gestion et supervision des téléphones à distance.

C'est pourquoi Alinéa a choisi d'utiliser SOTI.



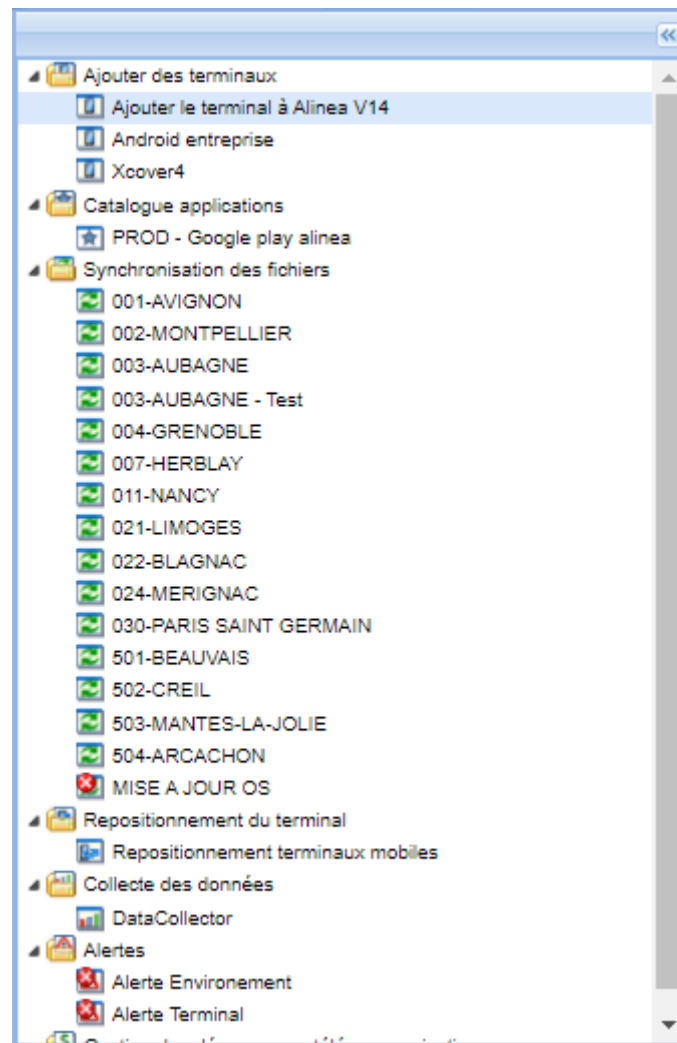
SOTI est une suite intégrée de solutions de mobilité pour l'entreprise. Elle permet aux utilisateurs de continuer à travailler, tout en créant nos applications plus rapidement et gérer nos périphériques mobiles et nos terminaux qu'ils soit mobile ou IoT.

L'installation sur les mobiles est simple puisqu'il suffit d'installer l'application Mobicontrolle sur les mobiles ou les PDAs et de connecter les téléphones à un réseau qui sera capable de communiquer avec le serveur qui contient le MDM de SOTI. C'est à partir du serveur SOTI que toutes les configurations se gèrent.

La gestion du MDM

Pour être efficace dans ma mission, j'ai dû me familiariser avec l'outil de Gestion de SOTI qui se présente sous la forme d'une Interface Web de gestion qui centralise la configuration des téléphones.

Tout d'abord les profils d'enrôlement :



On peut créer différents profils d' enrôlement en fonction de nos besoins. Par exemple, sur l' image ci-dessus, on peut voir les premières lignes « Ajouter le terminal à Alinéa » qui est la méthode de base d' enrôlement d' un téléphone.

Il existe ensuite des profils plus précis pour chaque magasin qui répondent à des demandes spécifiques.

On peut rajouter aux profils d' enrôlement des profils de gestion spécifique qui vont en plus rajouter un kiosque d' application à nos téléphones. Ainsi chaque téléphone enrôlé à partir du profil de base se verra attribuer, si on le souhaite, d' autres profils de gestion qui eux, vont leur permettre d' obtenir une adresse IP disponible de son sous réseau, les applications associés dans le kiosque, un certificat de sécurité, ainsi qu' une configuration pour se connecter automatiquement aux réseaux wifi autorisés.

Ma mission dans SOTI

Mon rôle était de simplifier et de nettoyer tous les profils de gestions spécifique, c'est à dire les profils qui permettent d'ajouter les applications, les certificats. En voici des exemples :

Attribué	TEST - Toutes les applications mobiles	Auto	42	0	2021-05-04 2:41:09 PM
Attribué	TEST - Kiosque	Auto	41	2	2021-03-25 5:24:31 PM
Attribué	PRODUCTION (ent.) - Toutes les applications mobiles	Auto	6	2	2021-04-29 11:48:04 AM
Attribué	PRODUCTION (ent.) - Paramètres	Auto	6	5	2021-05-06 11:05:40 AM
Attribué	PRODUCTION (ent.) - Certificats	Auto	2	1	2021-04-29 9:25:15 AM
Attribué	PRODUCTION - Toutes les applications mobiles	Auto	65	0	2021-05-17 6:29:48 PM
Attribué	PRODUCTION - Profil Wifi Alinea	Auto	6	1	2021-04-07 10:43:54 AM
Attribué	PRODUCTION - Kiosque	Auto	95	2	2021-04-07 10:43:58 AM
Attribué	PRODUCTION - Certificats	Auto	3	1	2021-04-29 9:22:45 AM

Nous avons deux environnements, un environnement de Test et un environnement de Production. Dès qu'une mise à jour d'un profil est nécessaire, elle est d'abord testée sur les environnements de Test avant d'être envoyée en Production. Cela nous permet d'avoir une meilleure vision des impacts liés au changement qu'apporte chaque mise à jour.

Voici un exemple d'un téléphone ayant bien reçu et installé les profils :

PHONE-00415

DÉTAILS DU TERMINAL

CONFIGURATIONS

APPLICATIONS

EMPLACEMENT

SÉCURITÉ

DONNÉES COLLECTÉES

JOURNAUX

<

>

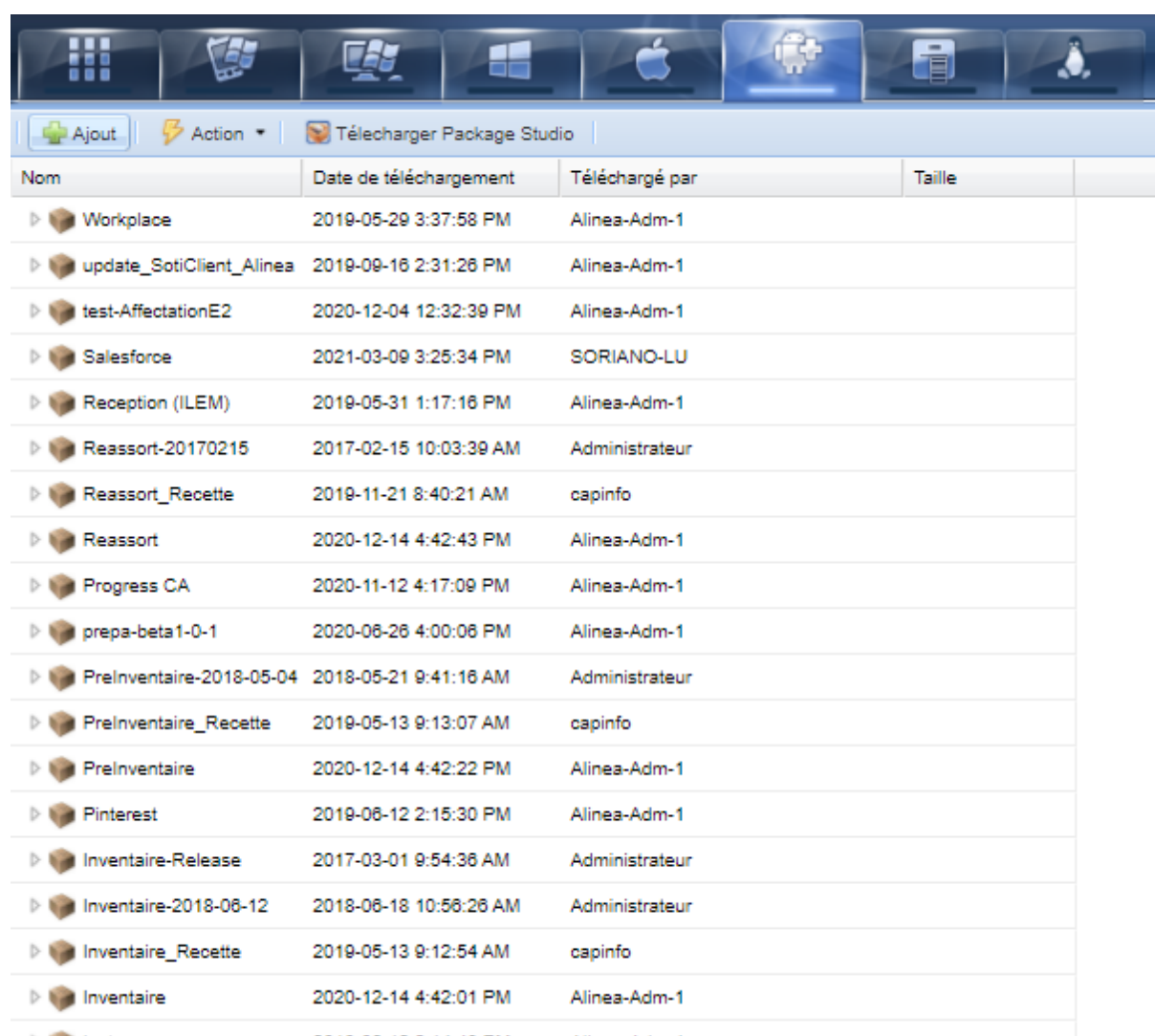
PROFILS

NOM DU PROFIL	ÉTAT	MÉTHODE INSTALL	VERSION	DATE D'ATTRIBUTION
> PRODUCTION - Certificats	● Installé	Automatique	3	2021-04-29 9:22:45 AM
> PRODUCTION - Kiosque	● Installé	Automatique	95	2021-04-07 10:43:58 A
> PRODUCTION - Profil Wi...	● Installé	Automatique	6	2021-04-07 10:43:54 A
> PRODUCTION - Toutes l...	● Installé	Automatique	65	2021-05-17 6:29:48 PM

La partie application

Pour gérer le déploiement des applications sur les téléphones, il faut d'abord récupérer les **APKs** des applications souhaitées. Une fois celles-ci récupérées, on utilise un MCStudio qui est un outil de SOTI qui permet de transformer son APK en Package et d'y ajouter des commandes supplémentaires. Par exemple, si je souhaite mettre à jour l'application Salesforce, je dois d'abord désinstaller Salesforce sur les téléphones avant d'installer la nouvelle version. C'est à ce moment qu'il nous suffit de rajouter dans les packages, les commandes de désinstallation de l'application et de lancer la commande avant l'installation.

Une fois le package créé, nous pouvons l'ajouter sur SOTI :



The screenshot shows the SOTI MCStudio interface. At the top, there is a navigation bar with icons for different operating systems: Windows, macOS, Linux, and Android. Below the navigation bar, there is a toolbar with buttons for 'Ajout' (Add), 'Action', and 'Télécharger Package Studio'. The main area displays a table of application packages.

Nom	Date de téléchargement	Téléchargé par	Taille
Workplace	2019-05-29 3:37:58 PM	Alinea-Adm-1	
update_SotiClient_Alinea	2019-09-16 2:31:26 PM	Alinea-Adm-1	
test-AffectationE2	2020-12-04 12:32:39 PM	Alinea-Adm-1	
Salesforce	2021-03-09 3:25:34 PM	SORIANO-LU	
Reception (ILEM)	2019-05-31 1:17:16 PM	Alinea-Adm-1	
Reassort-20170215	2017-02-15 10:03:39 AM	Administrateur	
Reassort_Recette	2019-11-21 8:40:21 AM	capinfo	
Reassort	2020-12-14 4:42:43 PM	Alinea-Adm-1	
Progress CA	2020-11-12 4:17:09 PM	Alinea-Adm-1	
prepa-beta1-0-1	2020-06-26 4:00:06 PM	Alinea-Adm-1	
PreInventaire-2018-05-04	2018-05-21 9:41:16 AM	Administrateur	
PreInventaire_Recette	2019-05-13 9:13:07 AM	capinfo	
PreInventaire	2020-12-14 4:42:22 PM	Alinea-Adm-1	
Pinterest	2019-06-12 2:15:30 PM	Alinea-Adm-1	
Inventaire-Release	2017-03-01 9:54:36 AM	Administrateur	
Inventaire-2018-08-12	2018-08-18 10:56:26 AM	Administrateur	
Inventaire_Recette	2019-05-13 9:12:54 AM	capinfo	
Inventaire	2020-12-14 4:42:01 PM	Alinea-Adm-1	

Listing d'un grand nombre de packages d'application. Chaque package doit ensuite être lié à un des profils que j'ai cité plus haut.

La partie Kiosque

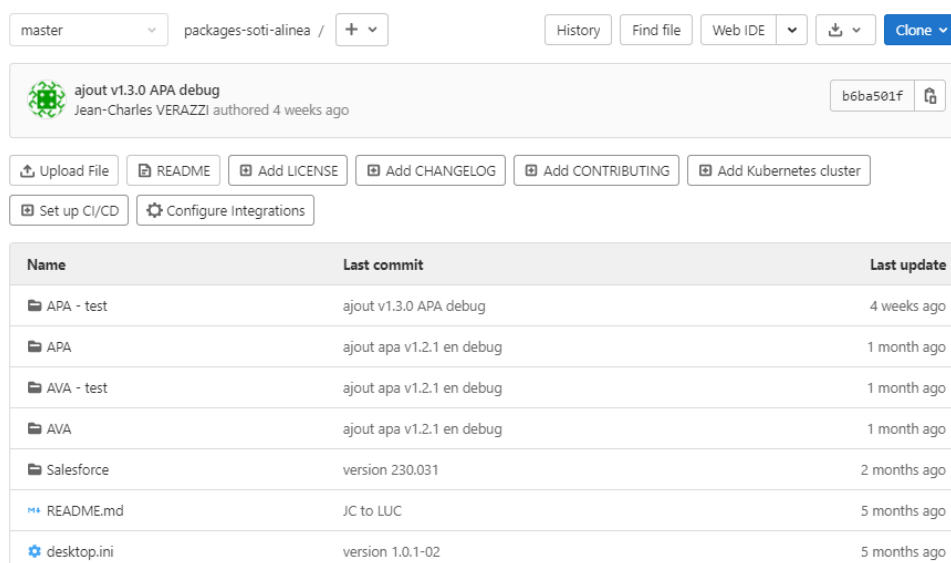
Le kiosque est à la fois une façon de verrouiller une partie des fonctionnalités des téléphones et d'uniformiser la présentation. Il est distribué via un profil qui est attribué ensuite aux téléphones exactement comme pour une application.

On peut gérer le kiosque directement sur SOTI via un outil de développement embeded, le langage que nous utilisons est le HTML

La méthodologie

Afin de ne pas se perdre, il a fallu réfléchir et développer une méthodologie stricte car de nombreuses contraintes de l'outil SOTI nous obligent à être attentif aux déploiements des package d'applications. À chaque nouveau build du package qui a lieu, à chaque mise à jour, une variable non visible du package est incrémentée de 1. SOTI n'autorise pas la mise à jour d'un package, si la variable du package à jour ne fait pas strictement partie de la suite logique croissante.

Ainsi pour ne pas se perdre dans les packages, nous avons proposé avec Jean-Charles Verrazzi d'utiliser un repo GitLab qui nous permet de stocker chaque paquet qui est géré par Alinéa et dont les mises à jour dépendent de l'équipe de développement interne. Voici un exemple du repo :



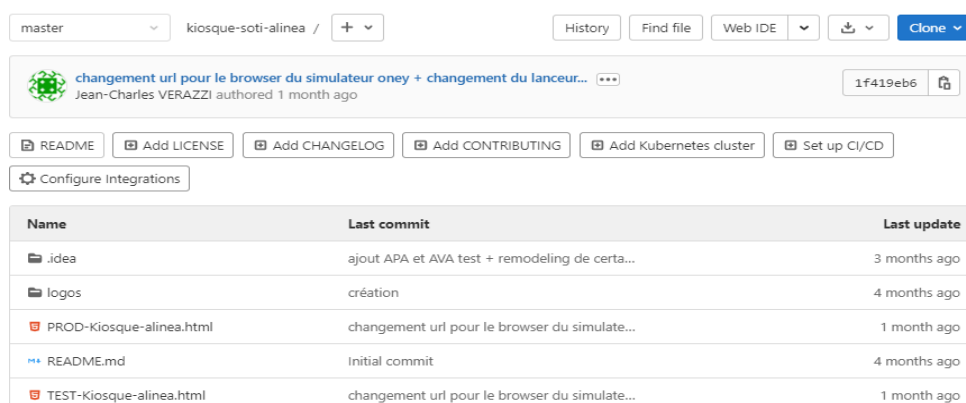
The screenshot shows a GitLab repository page for 'packages-soti-alinea'. At the top, there's a navigation bar with 'master' selected, a dropdown for 'packages-soti-alinea / +', and buttons for 'History', 'Find file', 'Web IDE', and 'Clone'. Below this, a commit summary shows 'ajout v1.3.0 APA debug' by 'Jean-Charles VERRAZZI' from '4 weeks ago' with the commit hash 'b6ba501f'. A row of buttons includes 'Upload File', 'README', 'Add LICENSE', 'Add CHANGELOG', 'Add CONTRIBUTING', and 'Add Kubernetes cluster'. Below these are 'Set up CI/CD' and 'Configure Integrations'. The main part of the image is a table listing repository contents.

Name	Last commit	Last update
APA - test	ajout v1.3.0 APA debug	4 weeks ago
APA	ajout apa v1.2.1 en debug	1 month ago
AVA - test	ajout apa v1.2.1 en debug	1 month ago
AVA	ajout apa v1.2.1 en debug	1 month ago
Salesforce	version 230.031	2 months ago
README.md	JC to LUC	5 months ago
desktop.ini	version 1.0.1-02	5 months ago

À partir du repo il ne reste plus qu'à pull le package, changer l'APK et re-build. Une fois le package mis à jour, il ne reste plus qu'à push les modifications et ainsi de suite.

Cette méthode étant très simple et très efficace, nous avons appliqué la même méthode pour les fichiers HTML du kiosque.

Voici un exemple du repo :



VOIP

Le sujet

En tant qu'enseigne d'ameublement, Alinéa doit être capable de répondre par téléphone à des clients si ceux-ci rencontrent des problèmes avec des commandes ou des produits. Alinéa possède également un service après-vente (SAV) qui prend en charge les incidents et les demandes des clients.

Depuis que je suis arrivé, j'ai été amené à me familiariser avec la VOIP de l'entreprise pour que je sois capable de gérer tous les problèmes liés à ceux-ci, je suis devenu le référent VOIP de l'entreprise.

Avant la crise sanitaire, la gestion était assez basique puisqu'il ne s'agissait que d'un simple support technique (changer les types de lignes etc ...) mais à l'annonce du confinement, de la fermeture des magasins et durant les longs mois de presque ouverture, de reconfinement additionnés au redressement judiciaire et la fermeture de plus de 17 magasins, le sujet est devenu très important.

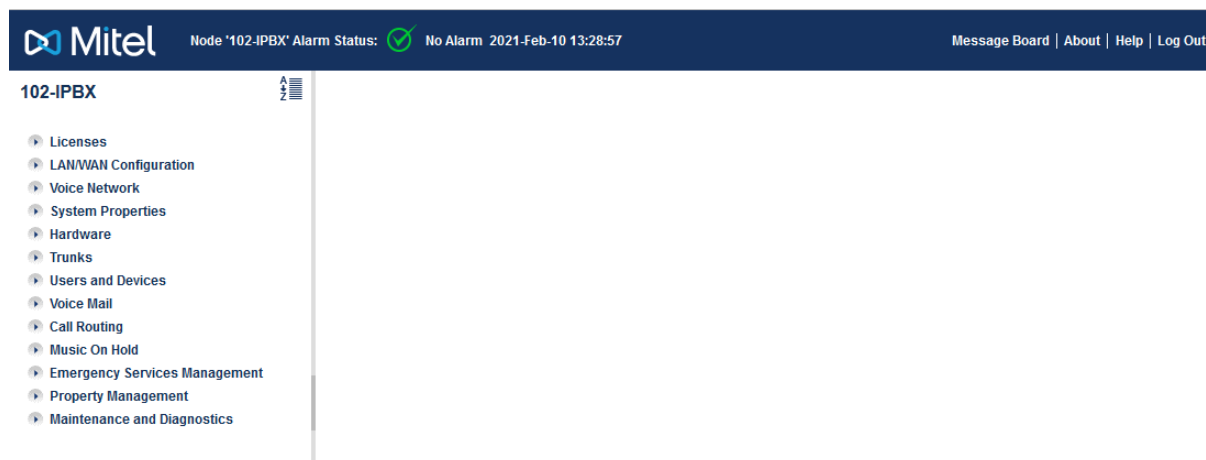
L'outil

Pour gérer la VOIP nous utilisons le service MITEL qui nous permet via l'utilisation d'IPBX de gérer la voix sur IP entre nos magasins ainsi que vers les lignes extérieurs.

Cet outil nous permet de gérer la téléphonie pour chaque magasin. Nous possédons donc 9 IPBX + 1 au siège donc 10 en tout. Chaque magasin possède sa propre interface de configuration.



Voici un exemple de la page d'accueil de l'interface Mitel pour un magasin :



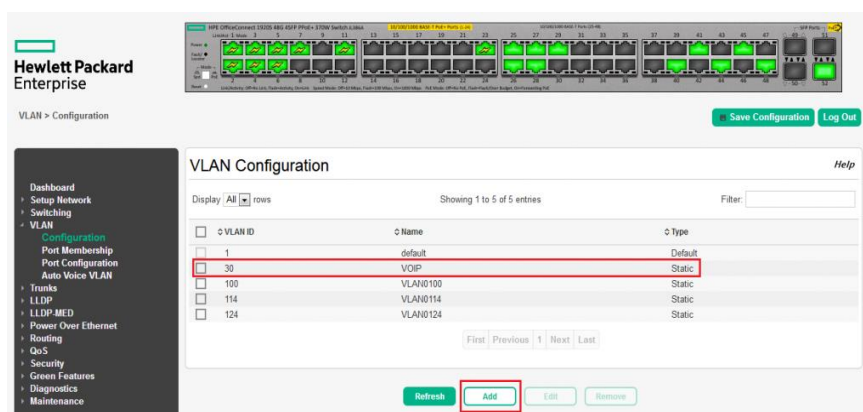
La Quality of Service (QoS)

Depuis la fermeture des magasins beaucoup de matériel informatique ont dû être retransférés rapidement vers les magasins qui resteraient ouverts. Certains des magasins qui ont fermé disposaient de matériels plus récents et de meilleure qualité, nous avons donc procédé à la modernisation de certains équipements, comme des téléphones mobiles, fixes ou encore les Switch HP.

C'est à ce moment que j'interviens, car le changement de switch a provoqué des problèmes au niveau de la configuration des VLANs. Je me suis donc occupé de la configuration des Switch pour intégrer une QoS.

La QoS permet d'identifier le trafic présent sur le Réseau. Ainsi on peut différencier le trafic VOIP, d'un trafic dit plus lourd comme des transferts de fichier.

J'ai d'abord penser qu'il fallait se connecter sur chaque switch pour y définir quelle interface serait dans le VLAN VOICE et que le trafic sera identifié comme VOIP. Voici un exemple (cette photo



n'est qu'une photo d'illustration très similaire au vrai switch que nous possédons, cependant les informations qui y serait affichées ne peuvent être dévoilées) :

Le problème avec cette méthode c'est qu'elle est très répétitive. C'est pourquoi, j'ai préféré rentrer la configuration en utilisant le **CLI** et ensuite récupérer cette

configuration et la transférer directement via WinSCP qui est un putty amélioré permettant de transférer des fichiers de configuration.

Voici comment j'ai rempli la configuration :

J'ai utilisé la commande system-view pour accéder au mode de configuration du switch.

```
# system-view
```

J'ai créé les VLANs, j'ai pris bien soin de séparer le VLAN data et le VLAN Voice afin d'identifier le trafic.

```
# vlan 1
# description Data Network
# quit
# vlan 200
# description Voice Network
# quit
```

J'ai sélectionné le port de l'IPBX et par la suite des téléphones, j'y ai ajouté la liste des VLANs autorisés.

```
# interface GigabitEthernet1/0/40
# voice vlan 200 enable
```

Les Mailboxes

Une fois les téléphones configurés, je dois définir le chainage des téléphones de chaque magasin dans l'outil MITEL, voici un exemple :

Node "102-IPBX" Alarm Status: ✔ No Alarm 2021-Feb-10 13:28:57

Message Board | About | Help | Log Out

102-IPBX

VM Mailboxes on 102-IPBX

DN to search

Show form on Not Accessible

Go

VM Mailboxes Search:

Find a field named: Mailbox Number that has a value of:

Search

Add Change Delete Print... Import... Export... Data Refresh

Mailbox Number	Name	Extension Number	Mailbox Type
0		0	Extension
2920	Choix 1	2920	Extension
6000	SVI	6000	Menu Node
2940	Choix 3	2940	Extension
4001	vers service client	2202	Transfer Only
2262	Choix 2	4000	Transfer Only
9999		9999	Administrator

Sur l'image ci-dessus on peut voir que les numéros de Mailbox (Mailbox number) qui sont les numéros d'identification des Mailboxes, sont associés à des extensions (Extension number) et ces extensions sont reliées à des numéros réels qui eux sont

joignables. Le but est donc de discuter directement avec les magasins pour savoir quelle ligne doit sonner quand une option est choisi par un client lors de l'appel du SVI (numéro principal du magasin).

Déménagement du datacenter

Contexte

Après le rachat d'Alinéa par Neomarche une décision a été prise par la direction, déplacer tous les serveurs physiques ainsi que les ESX et Nutanix de l'entreprise vers un hébergeur de cloud privé, pour des raisons de sécurité et afin de simplifier la gestion des futures évolutions. Un appel d'offre a été lancé afin d'identifier qui serait susceptible d'héberger nos infrastructures.

Trois entreprises ont répondu à l'appel d'offre. La négociation a duré plusieurs mois et l'entreprise retenue fut Jaguar Network.



Déroulé du déménagement

Dès l'entrée en fonction de Jaguar network, la priorité a été de définir les risques liés à l'arrêt de chaque service pendant la durée du déplacement des infrastructures (applications, données)

Le plan du déménagement a été défini par mon référent Stéphane Jeannot qui est le chef de projet technique sur ce sujet. Nous avons choisi de profiter de la fermeture des magasins due à la crise sanitaire pour que chaque action du déménagement n'affecte pas les performances de vente des magasins.

Une fois les risques évalués et le déroulé du déménagement défini, deux fiches techniques ont été réalisées. La première est l'ordre dans lequel les services devaient être arrêtés et le matériel éteint. Et la deuxième est l'ordre dans lequel ces services devaient être réinstallés et redémarrés.

Scénario du déménagement

Matériel :

Une liste du matériel à déplacer a été fourni avec les espaces et la consommation dans un **RACK** de chaque élément.

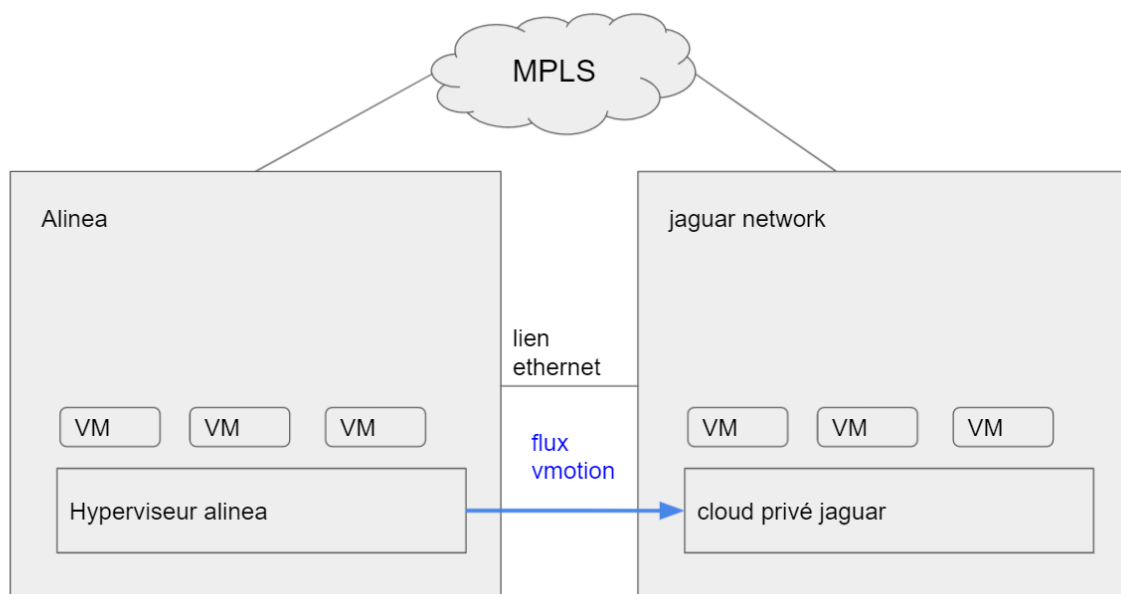
À noter que les baies SAN utilisent une connexion électrique différente (triphase) ainsi qu'un réseau fibre utilisant la technologie **Fiber Channel** entre elles.

Ces technos devaient donc être préparées à l'avance par Jaguar Network :

- Un lien fibre Fiber Channel entre les deux salles de l'hébergeur
- San switch pour la Baie de disque
- VLAN étendu entre deux salles de l'hébergeur pouvant fournir jusqu'à 10Go de débit
- La communication entre les serveurs Alinéa qui disposera toujours d'une infra réseau basique et l'infrastructure virtualisée

Réseau :

Les salles informatiques possèdent un lien réseau MPLS (ORANGE) et un lien internet (ORANGE). Ces deux liens doivent être redondés pour une meilleure sécurité.



Contraint par le temps, nous avons prévu de faire amener directement ces liens dans les salles informatiques de Jaguar Network, comme on peut le voir dans le schéma ci-dessus. Ainsi la transition des VM peut se faire à chaud via un flux Vmotion entre les deux salles.

L'étude de la possibilité de faire évoluer en services les firewall, Proxy, switch fournis par Jaguar Network est encore actuellement en étude mais n'est pas prévu avant

2022. Pour l'instant, l'infrastructure réseaux reste propriété Alinéa, exception faite pour le switch d'interconnexion.

Services attendus

Les services de base attendus par Alinéa étaient :

- La gestion des infrastructures des VM.
- Des services de supervision compatibles avec Windows 2003
- Une sauvegarde des VMs (sur 15 Jours + 1 sauvegarde persistante par an)
- Haute disponibilité des VMs
- Accès aux salles (sécurisation)
- Intervention sur site par Alinéa ou l'hébergeur
- Climatisation appropriée
- Alimentation constante et redondante avec protection par onduleur

Ma partie du déménagement.

Une autre de mes missions récurrentes est la supervision de la baie de disque du grand NAS HP. *Photo en annexe*

La supervision comprenait : La surveillance de l'espace disque disponible par **cluster** de disque, la commande de nouveaux disques directement à HP si un des disques tombait en panne et également la surveillance des chemins croisés qui relient la baie de disques et les deux fabriques (qui gèrent les 122 disques de la baie) au reste du réseau.

Pour le déménagement, j'ai superviser le déménagement de la baie de disques et de m'assurer du bon déroulement des opérations qui devaient s'effectuer par les prestataires d'Alinéa. Ainsi, j'ai dû prendre en compte tous les lecteurs virtuels et les ftp qui était reliés au NAS afin de définir un **PRA** permettant de s'assurer qu'au redémarrage des disques chaque lecteur soit de nouveau disponible et accessible et que les FTP pointent bien vers les nouvelles adresses IP internes de Jaguar Network. De plus, même si ce n'est pas moi qui me suis chargé du câblage de la baie, puisque ce sont les techniciens de Jaguar qui s'en sont chargés, j'ai dû vérifier que le câblage correspondait bien au même câblage qu'avant le déménagement et que celui-ci soit cohérent avec le plan d'interface du Switch Fibre d'interconnexion de chez Jaguar Network.

Les problèmes rencontrés

Lors du déménagement, la baie de disque a été éteinte, ce qui a causé le dysfonctionnement de certains disques durs qui ont dû être remplacés au redémarrage. Une fois les disques remplacés, j'ai dû me connecter sur les fabriques

pour déclarer l'ajout des deux disques et les associer au cluster correspondant. Une fois la tâche effectuée, la réparation des disques via le RAID 6 a pu s'enclencher.

Nous avons eu un autre problème au niveau des chemins croisés en fibre optique entre les fabriques et le switch fibre. Les impacts liés à cette erreur de synchronisation des chemins ne sont pas sans risque puisqu'elle empêche la répartition de charges de fonctionner, ce qui réduit la performance du réseau pour accéder aux données présentes sur le NAS. J'ai dû demander de l'aide afin de diagnostiquer le problème car il m'était inconnu et relevait d'un problème de protocole matériel qui était propriétaire à HP, et non d'une erreur réseau. Il s'est avéré qu'il s'agissait d'un problème de configuration au niveau de la synchronisation des interfaces croisées des Fabriques. Il a pu être résolu le lendemain grâce à l'intervention de Jaguar Network sous la supervision de Stéphane Jeannot.

Conclusion

Le déménagement s'est déroulé correctement et a pu s'effectuer rapidement et sans problème grave. Tout cela grâce à une excellente préparation de chacune des équipes impliquées. Au total, le déménagement aura duré deux semaines si l'on comptabilise le temps de chacun des acteurs du déménagement. Enfin, concernant ma participation, elle était répartie sur deux longues journées de 9 h de travail chacune.

Mise en place VPN pour MAC

Le VPN actuel utilisé par les MAC est utilisé par l'ensemble des utilisateurs à distance c'est-à-dire qu'ils comprennent également les utilisateurs de Windows. Le problème étant que pour s'authentifier au VPN il est nécessaire de posséder un compte dans l'AD. Cependant, un MAC ne peut s'authentifier via un Active directory que s'il y a un MAC serveur, ce qu'Alinéa ne possède pas. En conséquence, les utilisateurs de MAC avait trois mots de passes différents :

- Un mot de passe de leur session MAC
- Un mot de passe AD qui ne servait qu'à être connecté à L'AD
- Et le mot de passe GMAIL propre à chacun

Nous avons mis à profit le déménagement pour mettre en place un VPN unique pour les MACS, leur permettant ainsi d'utiliser le mot de passe de leur session, les utilisateurs Mac étant peu nombreux dans l'entreprise.

Pour le VPN, nous avons utilisé une solution clé en main gratuite limitée à deux utilisateurs. Il s'agit d'Open VPN AS. OpenVPN Access Server est une solution complète pour créer un tunnel privé grâce à OpenVPN.



L'administration se fait via une interface WEB, ce qui facilite la configuration et la gestion. Nous l'avons installé sur une machine virtuelle Debian, il est compatible avec la plupart des systèmes d'exploitation (MAC Os, Windows, Linux...).

Ce VPN est encore en test par les utilisateurs pour valider son bon fonctionnement. Il est destiné pour le moment à quatre utilisateurs sur une dizaine en tout.

L'avantage de ce VPN, par rapport à celui mis en place initialement pour les Macs, est qu'il permet de s'authentifier via sa session.

L'utilisation de plusieurs VPN reste cependant assez contraignant dans la gestion quotidienne car pour chaque modification à apporter, il faut faire les opérations deux fois. Malgré tout, cette opération reste en phase de test car les oublis de mots de passe sont assez fréquents.

VMWare et Active Directory

Le Sujet

En intégrant Alinéa en tant qu'administrateur Système et Réseaux, ma première missions fut de me familiariser avec son environnement Virtuel et le gestionnaire d'annuaire.

J'ai été épaulé par Stéphane Jeannot qui m'a beaucoup aidé à bien connaître le réseau ainsi que ses particularités.

La raison pour laquelle on m'a demandé d'être incollable sur ces environnements c'est parce qu'ils sont les fondations de tous les services utilisés par nos utilisateurs, puisque la plupart des applications fonctionnent à partir des VMs et que le gestionnaire d'annuaire fonctionne de pair avec le DHCP et le DNS.

Les outils

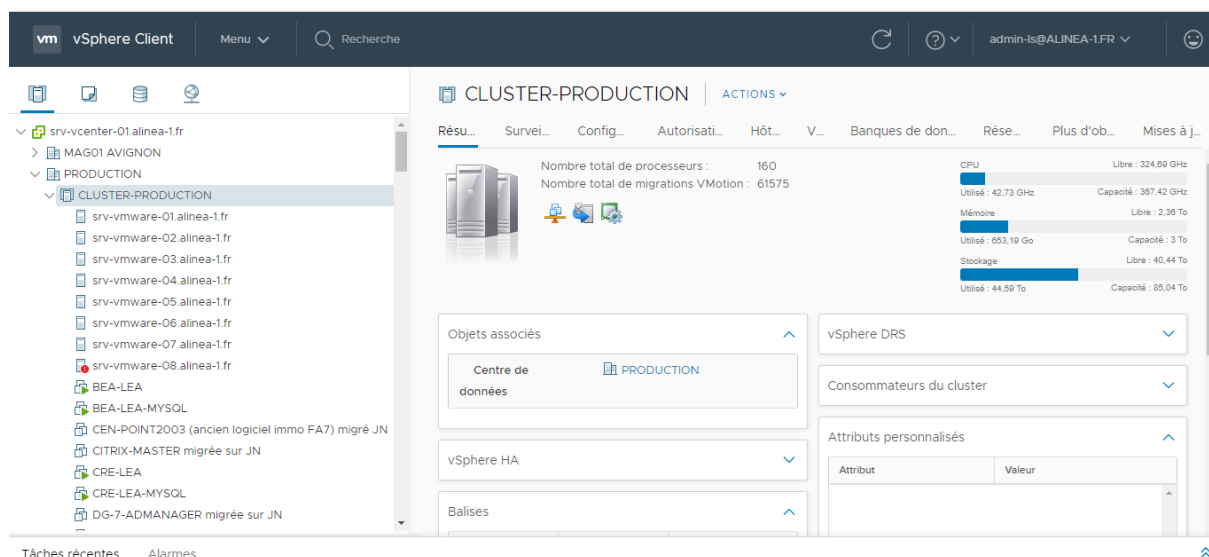
Le gestionnaire d'annuaire est Active Directory qui fonctionne sur un Windows 2012-R2. Très simple d'utilisation et compatible avec énormément de service. Voir schéma de fonctionne en annexe (5)
Je possédais déjà nombreuses compétences dans la gestion de ce service, mais j'ai pu encore les compléter avec les multiples associations possibles entre l'AD et des services comme le wiki, le VPN etc ...



Active Directory

Tout notre environnement virtuel est géré par VMWare, toutes nos VMs sont réparties entre plusieurs hyperviseurs VMWare. L'interface qui me permet de gérer toutes les VMs est VMWare Vsphere.

Cette interface est connue pour être très facile d'utilisation et très intuitive. Ainsi j'ai pu vite m'adapter à ce nouvel outil que j'avais légèrement survolé lors de mes précédents stages. Voici un exemple de l'interface de VMWare :



On peut voir ci-dessus le cluster de production qui regroupe tous les hyperviseurs d'alinéa dans lesquelles sont réparties toute les VMs de l'entreprise.

Schéma de fonctionnement en annexe (6)

Mes missions

Durant mes deux années à Alinéa, plusieurs projets ont dû être réalisés. Pour certains projets, la création ou l'utilisation de VMs était nécessaire. Ainsi, j'ai dû apprendre à vite être autonome sur cet outil, puisqu'il s'agit souvent de la première étape du sujet, que cela soit pour l'installation d'un service ou bien un moyen de faire des maquettes réseaux pour tester le déploiement d'une future infrastructure... J'ai dû également gérer les différentes alertes qui peuvent affecter les serveurs, comme des problèmes réseaux que ça soit un sur le routage ou un conflit d'IP... Il peut également y avoir des alertes sur les disques virtuels qui sont soit pleins ou « corrompus », ce qui peut indiquer qu'un des disques de la baie de disques est tombé en panne.

Conclusion

Vmware et Active Directory ont pris une place importante et quasi quotidienne parmi les outils que j'utilisais.

Il était donc très important d'acquérir une grande maîtrise de ces outils leader dans leur domaine, que je serais amené à utiliser très souvent dans mes futures missions.

Bilan

Le bilan sur l'ensemble de mon année au sein du service IT chez Alinéa a été très enrichissant pour moi.

Durant cette année, j'ai perfectionné mes connaissances et compétences en ayant intégré une grande équipe. Cela m'a permis d'apprendre des méthodologies de travail que je pourrais réutiliser lors de mes prochaines années.

Grâce à ces deux années d'alternance, la formation au sein d'Epitech m'a apporté des connaissances et compétences en matière de devops et de sécurité, nécessaires pour être efficace et opérationnel en entreprise. De plus, la partie entreprise m'a beaucoup apporté et confronté au milieu professionnel et ses exigences.

La gestion du parc informatique VM, ainsi que à la gestion du Parc Mobile faisaient partie des missions qui me prenaient le plus de temps. J'ai dû faire preuve d'imagination pour trouver le moyen d'automatiser la gestion de certaines actions ou du moins d'en faciliter leurs exécutions. Ces missions m'ont également obligé à la rigueur de devoir sans cesse fournir une documentation claire, nécessaire à un problème déjà rencontré et déjà résolu.

Le projet de déploiement du service Media-wiki m'a particulièrement intéressé et a conforté mes choix, m'orienter dans le devops et la sécurité. Un projet qui à la base devait s'apparenter à un simple clonage de service m'a permis, grâce aux connaissances acquises au sein d'EPITECH, de changer entièrement ma méthode d'approche.

Concernant la gestion de projet, j'ai dû apprendre à gérer la partie support en parallèle de mes autres projets. Cela m'a permis d'apprendre à bien maîtriser la gestion des priorités.

Les opérations de déménagement liées à la crise sanitaire ont été un véritable défi pour moi car elles avaient un impact réel, immédiat et très important pour l'entreprise. Celles-ci n'ont pas affecté les clients, mais ont eu un impact non négligeable sur les collaborateurs.

Il est important de souligner qu'un événement improbable comme la crise sanitaire que nous venons de vivre, a révélé le dynamisme de l'équipe IT. Sa réactivité et le travail effectué avec Jaguar Networks, ont permis de redéployer rapidement un nouvel environnement de travail plus abouti afin que l'entreprise Alinéa puis se relancer et perdurer.

Conclusion

J'ai passé deux années d'alternance chez Alinéa très enrichissante. J'ai intégré une entreprise de grande taille, avec les avantages et inconvénients que cela implique. Le principal inconvénient était le manque de réactivité sur certaines des prises de décision. Le principal avantage était la très grande variété de missions et les moyens financier affecté aux différents projets. Alinéa, récemment repris par Neomarche, est une entreprise chaleureuse où l'ambiance de travail est agréable. Les nombreux défis à relever, ont rendus les projets variés et intéressants.

J'ai effectué une importante montée en compétences au cours de ces deux années. Pour ce qui est du domaine technique, j'ai appris sur l'administration système, sur les technologies web, l'hébergement et la gestion de logiciel en mode SaaS. J'ai aussi enrichi ma maîtrise de l'anglais, utilisé pour la majorité des échanges au sein de l'entreprise. J'ai également travaillé sur le relationnel et mes aptitude a travailler en équipe, en m'intégrant et en collaborant avec la majorité des services.

Pour ce qui est de mes points faibles, j'évoquerai évidemment un manque de connaissances immédiates sur des technologies rencontrées, puisqu'il y avait quand même un grand nombre d'équipements qui m'était jusque-là inconnu. Je soulignerai aussi la difficulté à gérer parfois de front le travail sur un projet et la multitude de sollicitations extérieures (principalement support), ainsi qu'un manque d'expérience, notamment lors d'interventions nécessitant le contact avec plusieurs équipes.

Ces points faibles ont été, selon moi, compensés par ma persévérance, mon implication et ma force de proposition dans le différents projet.

Glossaire

VM : Virtual machine ou machine virtuel

Raid : La technologie RAID (Redundant Array of Inexpensive Disks) permet de constituer une unité de stockage à partir de plusieurs disques durs. L'unité ainsi créée (appelée grappe ou cluster) a donc une grande tolérance aux pannes (haute disponibilité), ou bien une plus grande capacité/vitesse d'écriture. La répartition des données sur plusieurs disques durs permet donc d'en augmenter la sécurité et de fiabiliser les services associés.

PDA : Un PDA (Personal Digital Assistant) est un ordinateur de poche composé d'un processeur, de mémoire vive, d'un écran tactile et de fonctionnalités réseau dans un boîtier compact d'extrêmement petite taille.

APK : est un format d'exécutable pour les téléphones qui possède un OS Android.

RACK : Un rack est une armoire très souvent métallique parfois à tiroirs mais généralement à glissières (ou rails) destinée à recevoir les boîtiers d'appareils, généralement électroniques, réseau ou informatiques de taille normalisée.

CLI : interface de ligne de commande

Bibliographie

<https://fr.wikipedia.org/wiki>

<https://www.cit-devops.com>

www.google.com

www.alinea.fr

<https://forums.macg.co>

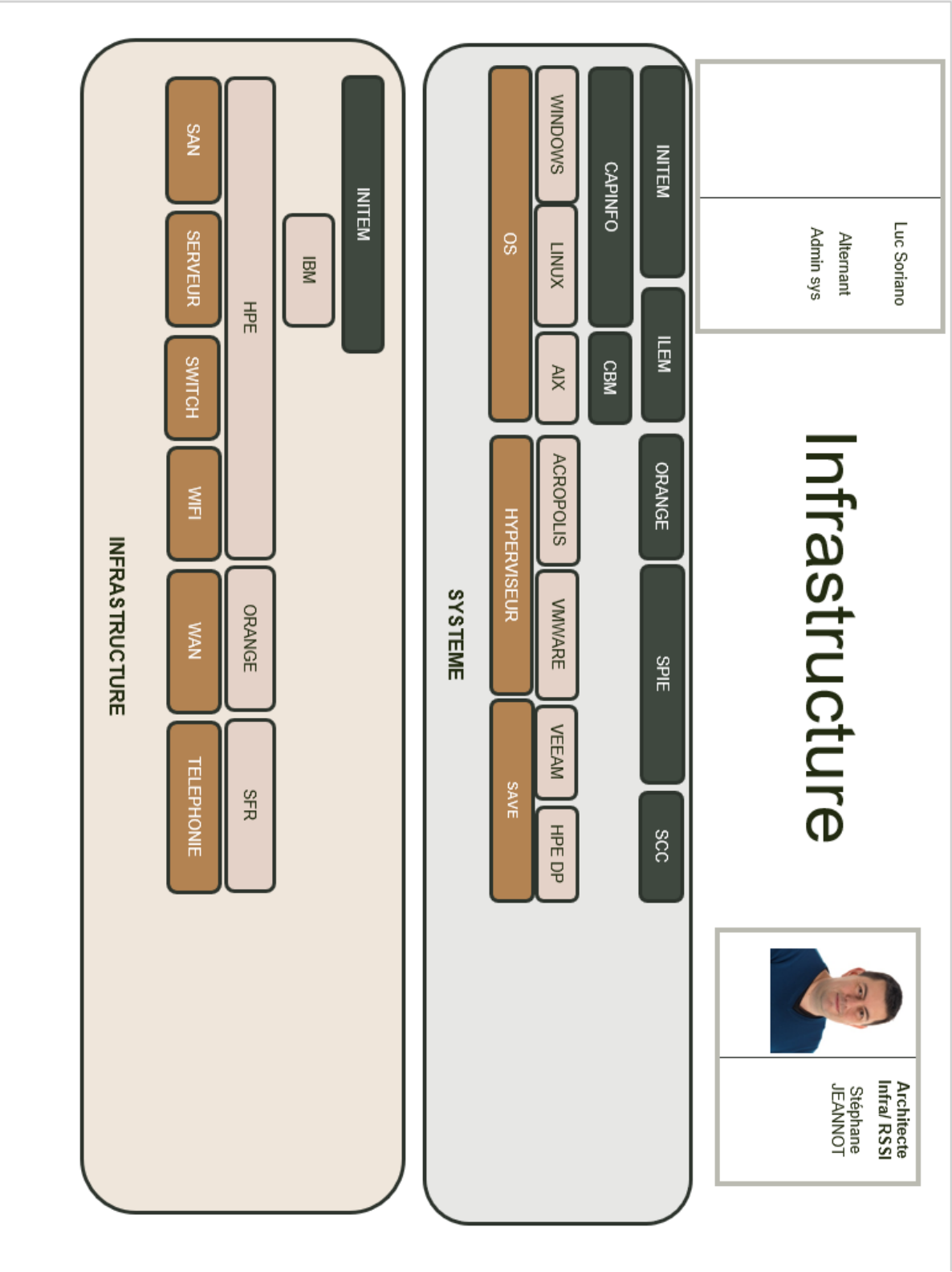
<https://openclassrooms.com/>

<https://www.commentcamarche.net/>

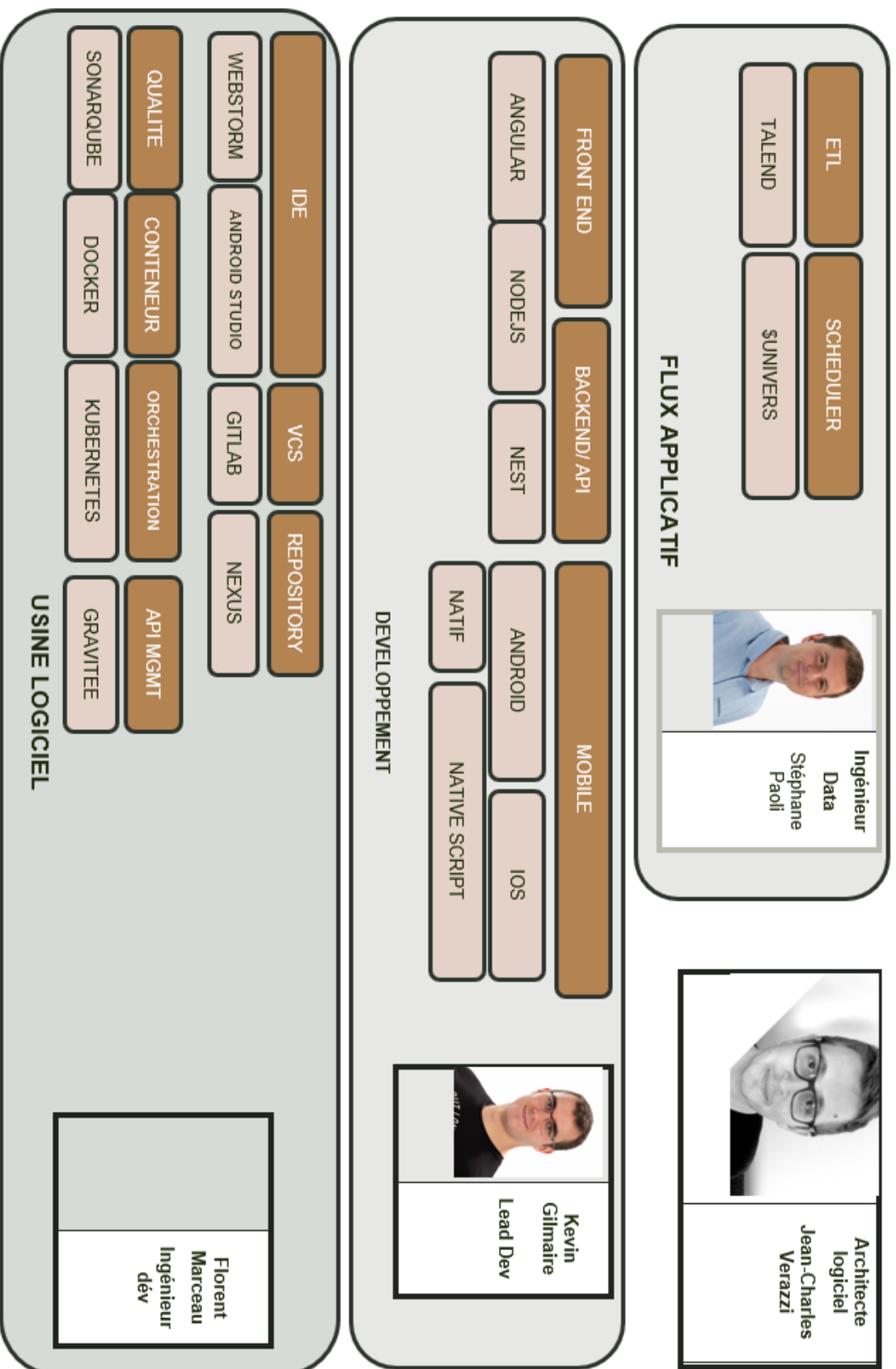
Toutes les ressources internes à Alinéa

Annexes

Annexe 1 : Organigramme Infrastructure



Logiciel

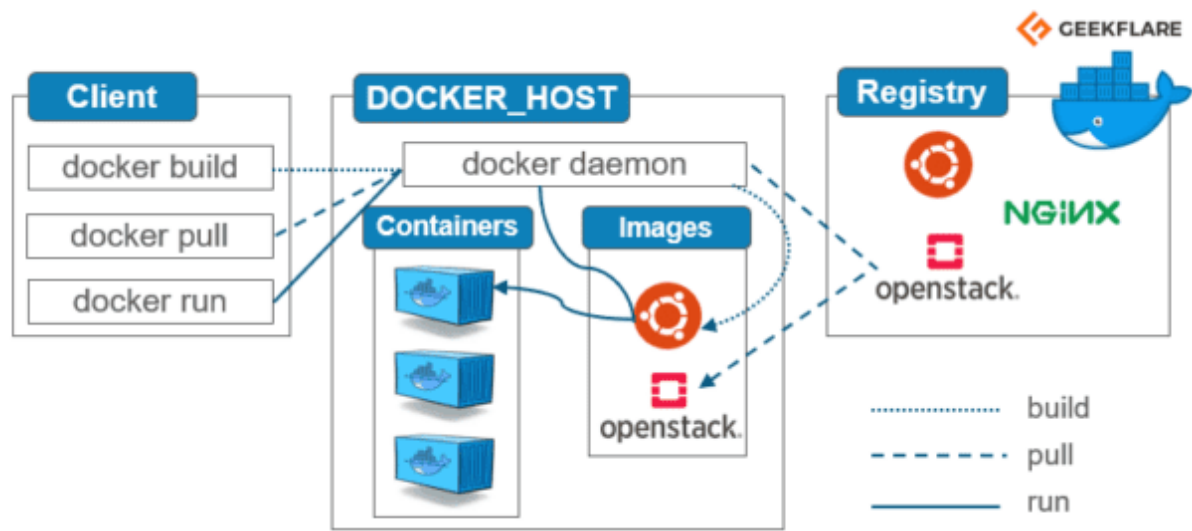


Annexe 2 : Organigramme Logiciel

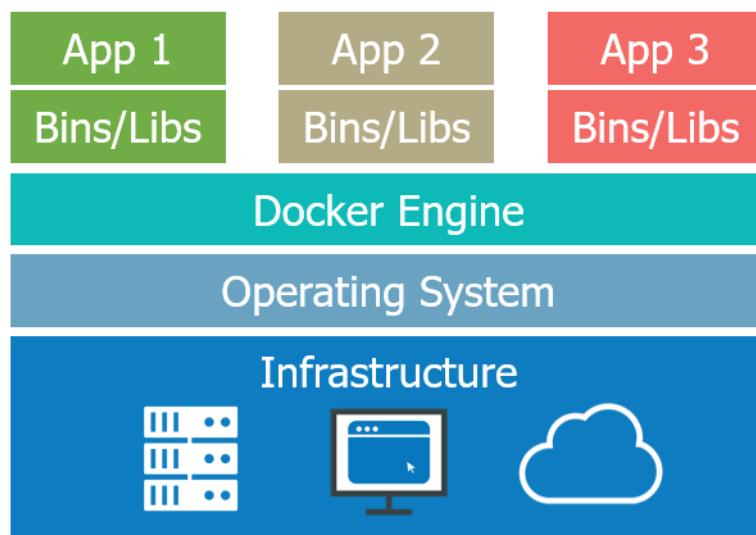
Annexe 3 : Script Powershell

```
1 | Import-Module ActiveDirectory
2
3 #Cr ation des warnDates pour les expirations de mot de passe future
4 $FifteenDayWarnDate = (get-date).adddays(15).ToLongDateString()
5 $SevenDayWarnDate = (get-date).adddays(7).ToLongDateString()
6 $ThreeDayWarnDate = (get-date).adddays(3).ToLongDateString()
7 $OneDayWarnDate = (get-date).adddays(1).ToLongDateString()
8
9 #variables email
10 $Username = "██████████"
11 $Pwd = ConvertTo-SecureString "██████████" -AsPlainText -Force
12 $SMTPCred = New-Object System.Management.Automation.PSCredential ($Username, $Pwd)
13 $SMTPCred = (get-credential)
14 $MailSender = "robot@██████████"
15 $SMTPServer = "smtp.office365.com"
16 $SMTPPort = "587"
17 $encodingMail = [System.Text.Encoding]::UTF8
18
19 $ToIT = "██████████"
20 $SubjectIT = "PwdExpWarning : 3-1 pour"
21
22 $SubjectUser = "ATTENTION ! votre mot de passe expire dans"
23 $BodyUser = "COMMENT LE R  CHANGER ?"
24 -  tre dans un bureau ██████████ et connect  au r seau (soit par c ble, soit par WiFi)
25 - aller dans le menu suivant...
26   MAC users : POMME / "Pr f rences Syst me" / "utilisateurs et groupes" / "modifier mot de passe"
27   WINDOWS users : CTRL+ALT+SUPPR / "modifier mot de passe"
28 - le nouveau mot de passe DOIT :  tre d'au moins 8 caract res (majuscules ET minuscules ET chiffres)
29 - le nouveau mot de passe ne doit PAS : comporter de caract res sp ciaux ('  ', '  ', '  ', '  ', '  ', '  ', '  ', '  '), ni  tre identique   un mot de passe pr c demment utilis 
30
31 Pour m mo : votre nouveau mot de passe sera valable 3 mois.
32 Si les rappels par mail ne vous conviennent pas...
33   MAC users : vous pouvez afficher un petit compteur indiquant le nombre de jours restants avant la prochaine expiration en installant ce soft : https://files.nomad.nenu/NOMAD.pkg
34   Windows users : votre syst me vous notifie nativement du nbr de jours restants
35
36 En cas de doute ou de difficult , avant/pendant/apr s ce changement de mot de passe, l' quipe IT se tient   votre disposition."
37
38 #Trouve les comptes qui sont actifs et qui ont un mot de passe "PAS illimit "
39 $users = Get-ADUser -filter (Enabled -eq $true -and PasswordNeverExpires -eq $false -and PasswordLastSet -gt 0)
40 -Properties "Name", "EmailAddress", "msDS-UserPasswordExpiryTimeComputed" | Select-Object -Property "Name", "EmailAddress",
41  (Name = "PasswordExpiry"; Expression = [[datetime]::FromFileTime($_.msDS-UserPasswordExpiryTimeComputed)].toLongDateString()) }}
42
43 #Envoie le mail pour chaque user en fonction des warnDates
44 foreach ($user in $users) {
45     if ($user.PasswordExpiry -eq $FifteenDayWarnDate) {
46         $days = 15
47         $EmailBody = $BodyUser -join ' '
48         $EmailTitle = $SubjectUser, $days, "jours" -join ' '
49
50         Send-MailMessage -To $user.EmailAddress -From $MailSender -Subject $EmailTitle -SmtpServer $SMTPServer -Body $EmailBody -Port $SMTPPort -UseSsl -Credential $SMTPCred -Encoding $encodingMail
51     }
52     elseif ($user.PasswordExpiry -eq $SevenDayWarnDate) {
53         $days = 7
54         $EmailBody = $BodyUser -join ' '
55         $EmailTitle = $SubjectUser, $days, "jours" -join ' '
56
57         Send-MailMessage -To $user.EmailAddress -From $MailSender -Subject $EmailTitle -SmtpServer $SMTPServer -Body $EmailBody -Port $SMTPPort -UseSsl -Credential $SMTPCred -Encoding $encodingMail
58     }
59     elseif ($user.PasswordExpiry -eq $ThreeDayWarnDate) {
60
61         $EmailBody = $BodyUser -join ' '
62         $EmailTitle = $SubjectUser, $days, "jours" -join ' '
63         Send-MailMessage -To $user.EmailAddress -From $MailSender -Subject $EmailTitle -SmtpServer $SMTPServer -Body $EmailBody -Port $SMTPPort -UseSsl -Credential $SMTPCred -E
64     }
65     elseif ($user.PasswordExpiry -eq $OneDayWarnDate) {
66         $days = 1
67         $EmailBody = $BodyUser -join ' '
68         $EmailTitle = $SubjectUser, "demain !" -join ' '
69         Send-MailMessage -To $user.EmailAddress -From $MailSender -Subject $EmailTitle -SmtpServer $SMTPServer -Body $EmailBody -Port $SMTPPort -UseSsl -Credential $SMTPCred -E
70         $EmailTitleIT = $SubjectIT, $user.name -join ' '
71         Send-MailMessage -To $ToIT -From $MailSender -Subject $EmailTitleIT -SmtpServer $SMTPServer -Port $SMTPPort -UseSsl -Credential $SMTPCred
72     }
73     else {}
74 }
75
76
```


Annexe 4 : fonctionnement Docker



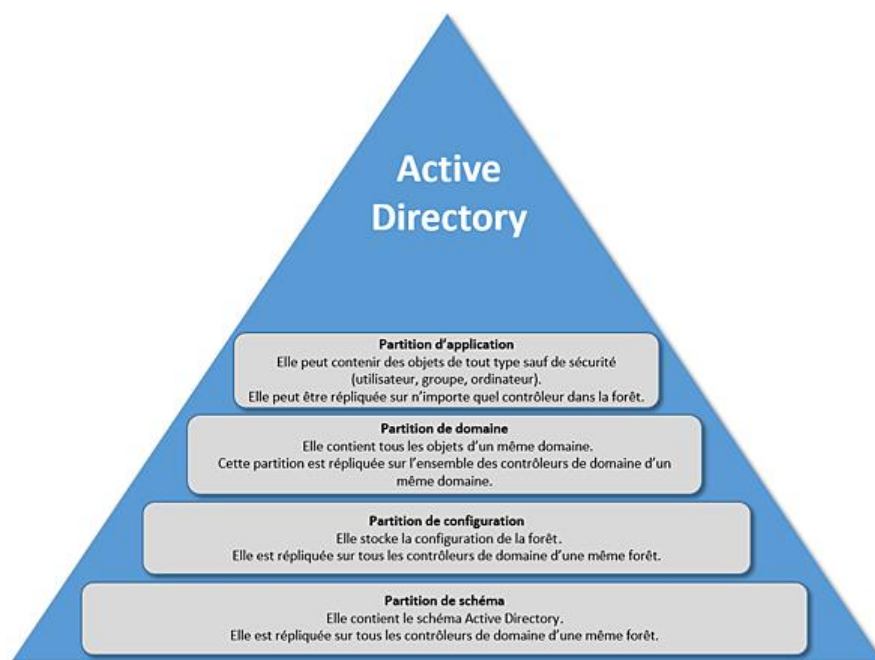
Container :



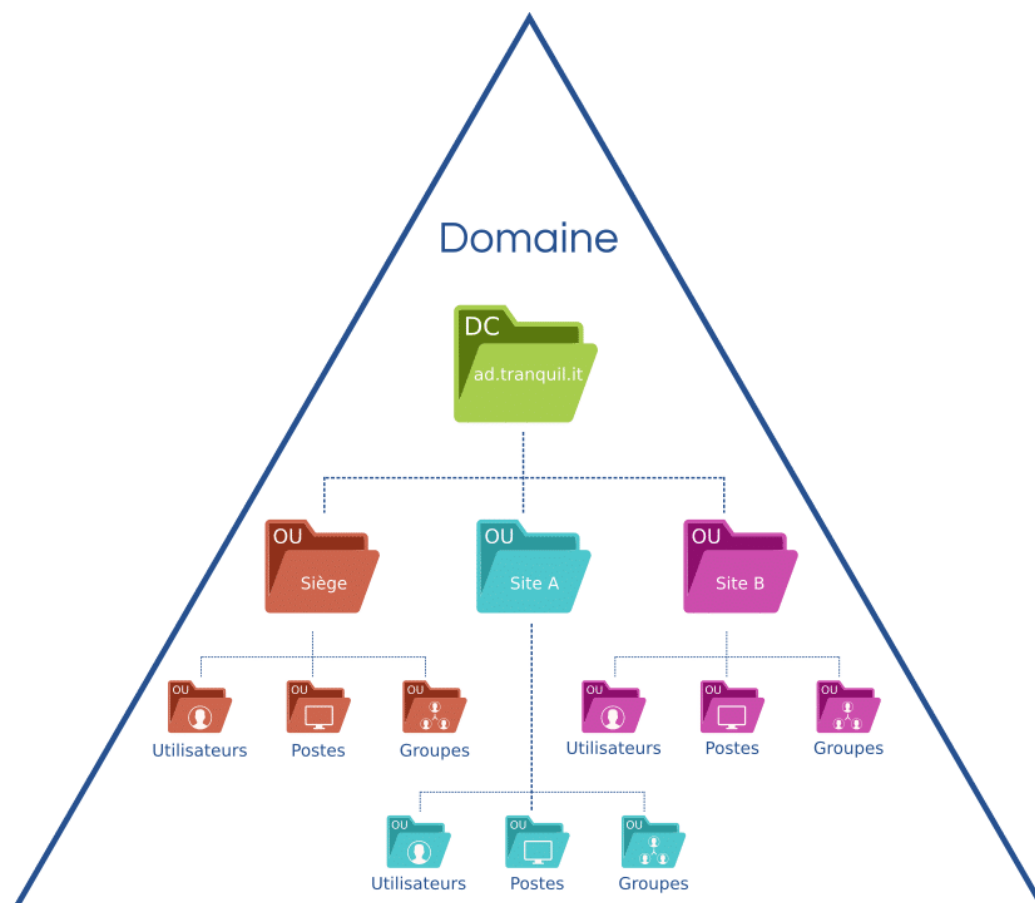
Annexe 5 : Baie de disque



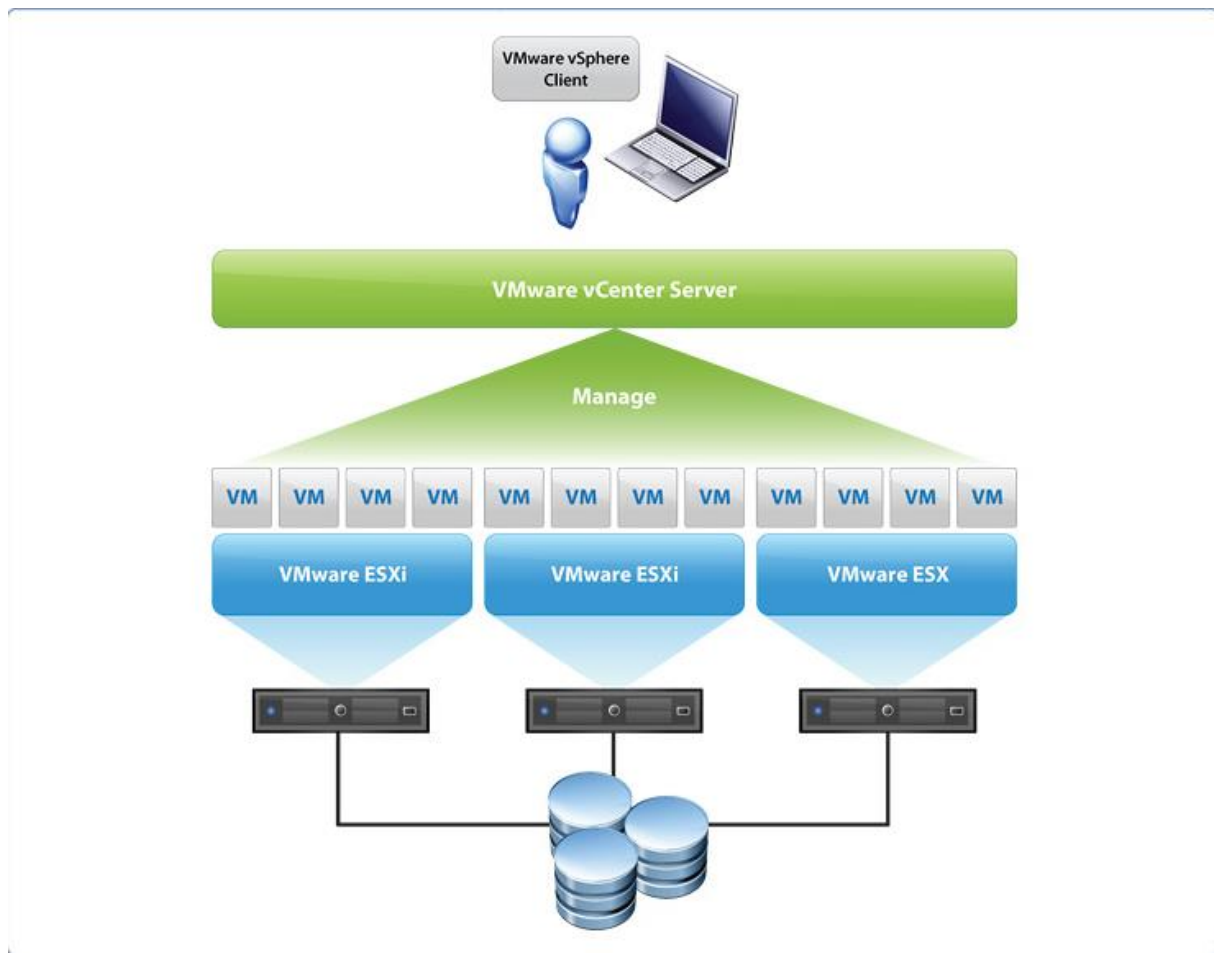
Annexe 6 : Fonctionnement Active Directory



Fonctionnement domaine AD :



Annexe 6 : Fonctionnement VMWare



Zoom sur les VMs :

