



CONSEIL & INGENIERIE INFORMATIQUE



**REPONSE COMMERCIALE :
Refonte de l'architecture Active
Directory**



Microsoft®
GOLD CERTIFIED
Partner

Table des Matières

1. PRESENTATION DE LA SOCIETE (Nicolas)
 - 1.1. Historique
 - 1.2. Quelques chiffres
 - 1.3. Notre proposition de valeur
 - 1.4. Notre engagement face à vos enjeux
2. OBJET DU DOCUMENT (Nicolas)
 - 2.1. Contexte
 - 2.2. Périmètre et limites
 - 2.3. Présentation du document
3. DESCRIPTIF DES BESOINS (Jonathan)
 - 3.1. Compréhension du besoin fonctionnel
 - 3.2. Compréhension du périmètre technique
 - 3.3. Synthèse des besoins
4. ETAT DE L'EXISTANT (Jonathan)
 - 4.1. Infrastructure réseau
 - 4.2. Infrastructure Active Directory existante
 - 4.3. Relevé des OU
5. SOLUTIONS PROPOSEES
 - 5.1. Infrastructure réseau (Alexis)
 - 5.2. Infrastructure Active Directory proposé
(Alexis partie 1 et 2 & Nicolas partie 3 et 4)
 - 5.3. Virtualisation (Mahmoud)
 - 5.4. Cloud (Mahmoud)
 - 5.5. PCA / PRA (Alexis)
 - 5.6. Sauvegarde (Alexis)
6. PLANNIFICATION DU PROJET (Nicolas)
7. EVALUATION FINANCIERE (Nicolas)
8. CONCLUSION (Jonathan)

1. PRESENTATION DE LA SOCIETE

1.1. Historique

Créée en 1990, **IZI'T** est une société d'ingénierie informatique spécialisée dans les technologies Microsoft.

La proximité géographique de son siège social avec celui de Microsoft France, accélère le partenariat avec l'éditeur et tisse, entre **IZI'T** et Microsoft France, des liens de confiance qui perdurent jusqu'à aujourd'hui.

Dès sa création, **IZI'T** développe en avance de phase ses compétences sur dernières solutions de Microsoft.

Au départ détenu à 100% par un actionnariat privé, en août 2010, **IZI'T** intègre Orange en devenant une filiale à 100% du Groupe France Telecom.



1.2. Quelques chiffres

1.2.1.Chiffre d'affaire

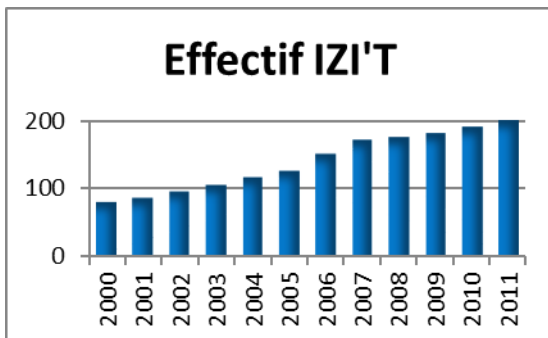
Depuis de nombreuses années le chiffre d'affaire de IZI'T est en croissance constante.



2006	11,5M€ dont 12,5% hors France
2007	14 M€ dont 15% hors France
2008	15,3M€ dont 15% hors France
2009	15,5M€ dont 15% hors France
2010	19 M€
2011	21 M€

1.1.1.Effectifs

L'effectif globale de IZI'T est d'environ 200 collaborateurs et est en constante augmentation.



2006	150 personnes	au 31/12/2006
2007	170 personnes	au 31/12/2007
2008	175 personnes	au 31/12/2008
2009	180 personnes	au 31/12/2009
2010	190 personnes	au 31/12/2010
2011	200 personnes	au 31/12/2011

		RFONTE DE L'ARCHITECTURE AD		VERSION 2.0	DATE 22/02/13
--	--	--------------------------------	---	-----------------------	-------------------------

1.2. Notre proposition de valeur

Depuis sa création, IZI'T démontre sa capacité à croître de façon constante et raisonnée. Sa pérennité depuis plus de 20 ans fait aujourd'hui de IZI'T une filiale autonome et financièrement indépendante d'Orange.

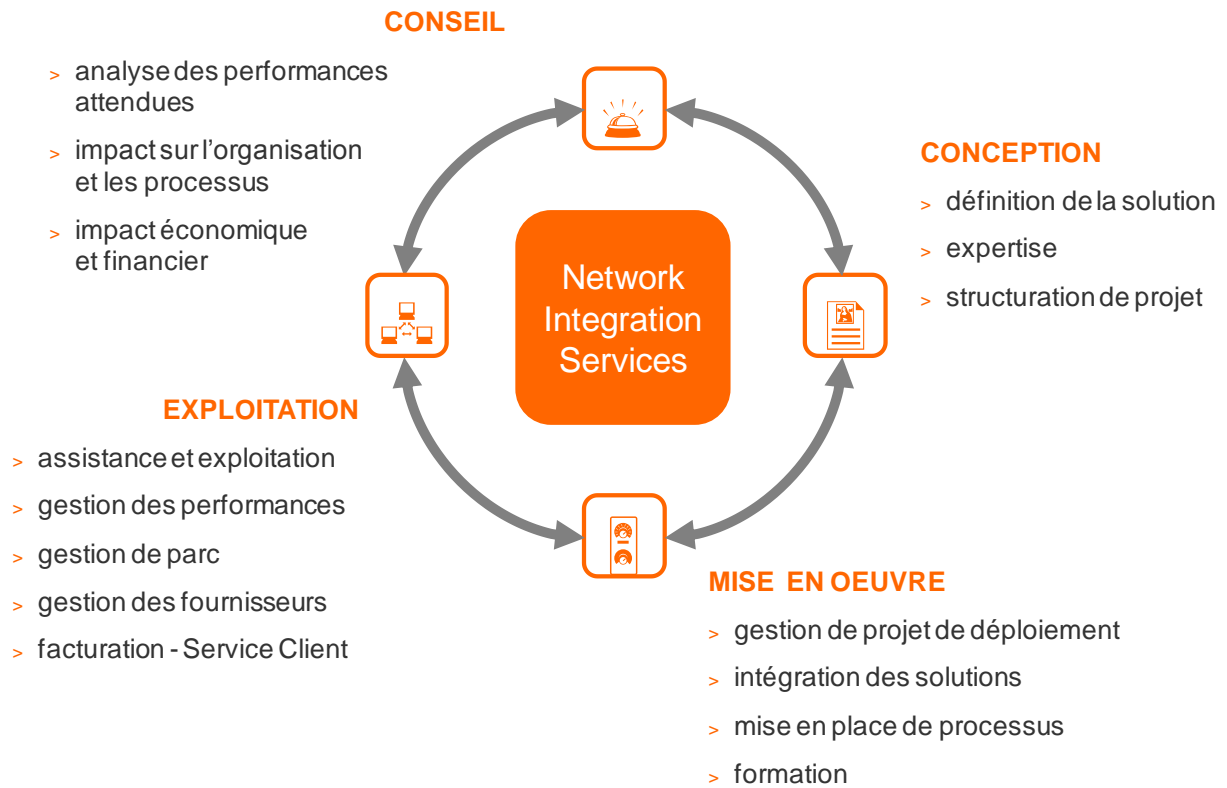
En tant que filiale IZI'T donne une véritable valeur ajoutée aux offres du groupe et apporte le liant pour la convergence entre les télécoms et les systèmes d'information Microsoft de ses clients.

Positionné en tant que partenaire Microsoft historique et privilégié, IZI'T est toujours en avance de phase sur les dernières solutions de Microsoft et vise à rester à la pointe des technologies innovantes développées par l'éditeur.



1.3. Notre engagement face à vos enjeux

Nous appuyons notre expertise sur nos savoir-faire techniques, notre capacité de gestion de projets d'envergure, stratégiques et structurants.



2. OBJET DU DOCUMENT

2.1. Contexte

L'acquisition des entreprises Wingtip Toy et Contoso Ltd mais et les nouveaux accords partenariaux avec Trey Research, A. Datum Corporation et Consolidated Messenger ont amené de nouvelles problématiques d'authentification et d'accès.

Le présent document est une réponse d'avant-vente liée à votre appel d'offre.

Il a pour objectif de vous donner nos réponses face à vos besoins concernant la consolidation de votre annuaire d'entreprise.

2.2. Périmètre et limites

Ce document décrit de manière globale la réponse au cahier des charges. Celui-ci ne donne aucune indication de planification détaillée des tâches à réaliser.

2.3. Présentation du document

Ce document est décomposé en cinq grandes parties :

- ✓ Analyse des besoins
- ✓ Architecture de l'existant
- ✓ Architecture de la solution proposée
- ✓ Procédures et technologie de sécurité
- ✓ Méthodologies d'administration

3. DESCRIPTIF DES BESOINS

3.1. Compréhension du besoin fonctionnel

3.1.1. Avant-propos

Vous trouverez ci-dessous la réponse à l'appel d'offres, notre société a résumé les besoins exprimés par l'équipe de Tailspin Toys™.

Ce résumé est à considérer comme réponse à un appel d'offres et définit le périmètre de l'engagement de notre société

3.1.2. Besoins fonctionnels

- ✚ Consultation pour la conception et la hiérarchisation d'une architecture Active Directory.
- ✚ Faciliter l'administration de l'Active Directory.
- ✚ Renforcer le niveau d'authentification.
- ✚ Faciliter les communications et les échanges entre les différents éléments du groupe
- ✚ Sécurisation du réseau interne, intersites et vers internet.
- ✚ Sécurisation des répliqués Active Directory.
- ✚ Conseils pour l'ajout de fonctionnalité de virtualisation,
- ✚ Haute disponibilité,
- ✚ Tolérance de pannes,
- ✚ Redondance.
- ✚ Solution de stockage réseau,
- ✚ Modification du réseau interne impacté.

3.2. Compréhension du périmètre technique

Suite à l'évolution de la société Tailspin Toys, cette dernière s'organise de cette façon :

Le siège social de l'entreprise principale Tailspin Toys est basé à New York et sa nouvelle filiale de production et distribution à Fayetteville.

Wingtip Toys avec deux sites (Houston et Austin) et Contoso Ltd avec deux sites également (Palo Alto et San Ramon) sont des nouvelles entreprises spécialisées dans les jeux électroniques.

A celle-ci s'ajoute un partenariat avec trois fournisseurs. Certaines informations au sein de Tailspin Toys devront être accessibles à ces fournisseurs.

Le schéma ci-dessous regroupe les différentes filiales de Tailspin Toys, leurs utilisateurs et leurs fournisseurs.



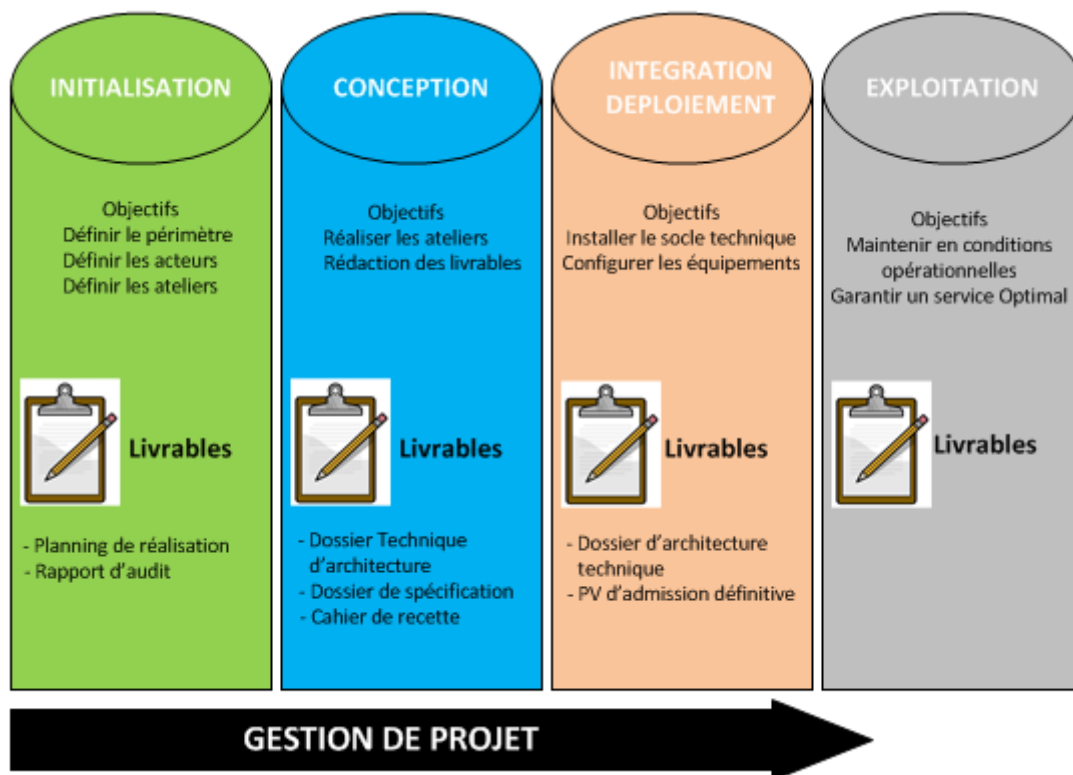
3.3. Synthèse des besoins

Pour résumer concrètement vos besoins, la principale requête est de simplifier l'administration tout en maintenant une forte authentification, sans oublier de proposer de nouvelles solutions afin de contrôler la charge induite par les nouvelles filiales et l'expansion de l'étendu de l'activité professionnelle.

Il faut également prévoir les évolutions de l'entreprise, comme les emplois futurs en prévision d'une augmentation de l'activité.

Le groupe Tailspin Toys™ souhaite également faciliter les accès et les échanges entre ces partenaires (Trey Research & A. Datum Corporation).

Le périmètre impacté par ces besoins sera décrit puis notre société vous proposera des solutions afin de répondre au mieux à ces besoins. Pour ce faire, nous nous appuyons sur le modèle de gestion de projet ci-dessous.



4. ETAT DE L'EXISTANT

Le finalité de cette partie du document est de reconstituer succinctement, l'infrastructure de Tailspin Toys™ et de ces filiales, à la fois au niveau de l'infrastructure réseau et au niveau de l'architecture Active Directory mais aussi de ces interactions avec ses fournisseurs ou prestataires de services, à partir des informations transmises.

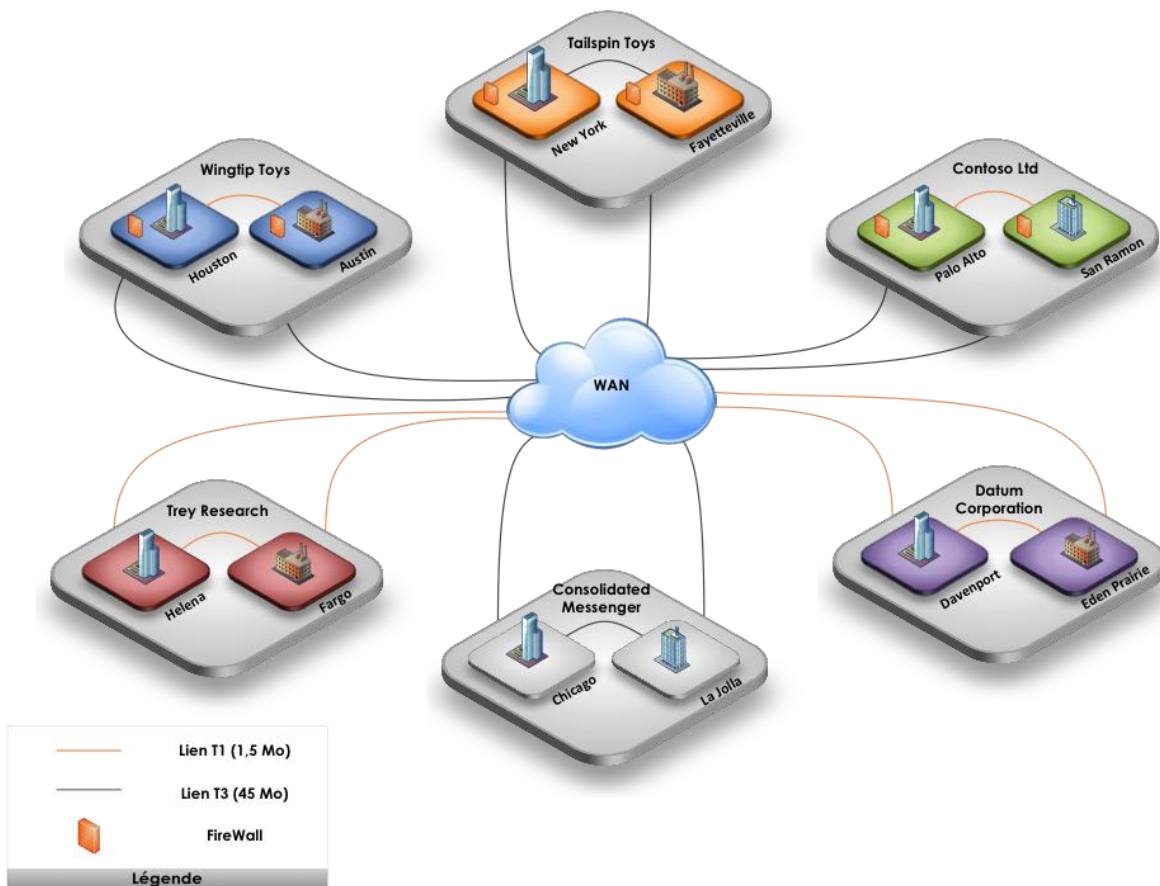
4.1. Infrastructure réseau

Tailspin Toys™ est réparties sur 6 sites qui sont interconnectés via le réseau internet public. Ces sites interagissent les uns avec les autres, ces échanges se sont densifiés et multipliés depuis le rachat des sites Contoso Ltd™ et Wingtip Toys™.

De nombreuses communications s'effectuent également avec le réseau des fournisseurs et des prestataires de services de gestion des ressources humaines. Le périmètre étant établi, cela sera plus simple de présenter une base de communication entre ces différentes entités.

Les débits des interconnexions sont à prendre en compte pour le projet de conception d'architecture Active Directory. Seules les interconnexions et les accès de ces entreprises avec Tailspin Toys™ sont prises en comptes.








Les débits des interconnexions sont à prendre en compte, afin de ne pas corrompre les processus de réplication des différents contrôleurs de domaine, ainsi que les échanges de fichiers sécurisés ou consultation de diverses ressources.

Une fois l'infrastructure réseau assimilée, il sera plus simple de prendre en compte les différentes relations ayant un rapport avec l'infrastructure et d'en estimer l'impact sur les liens opérateurs.

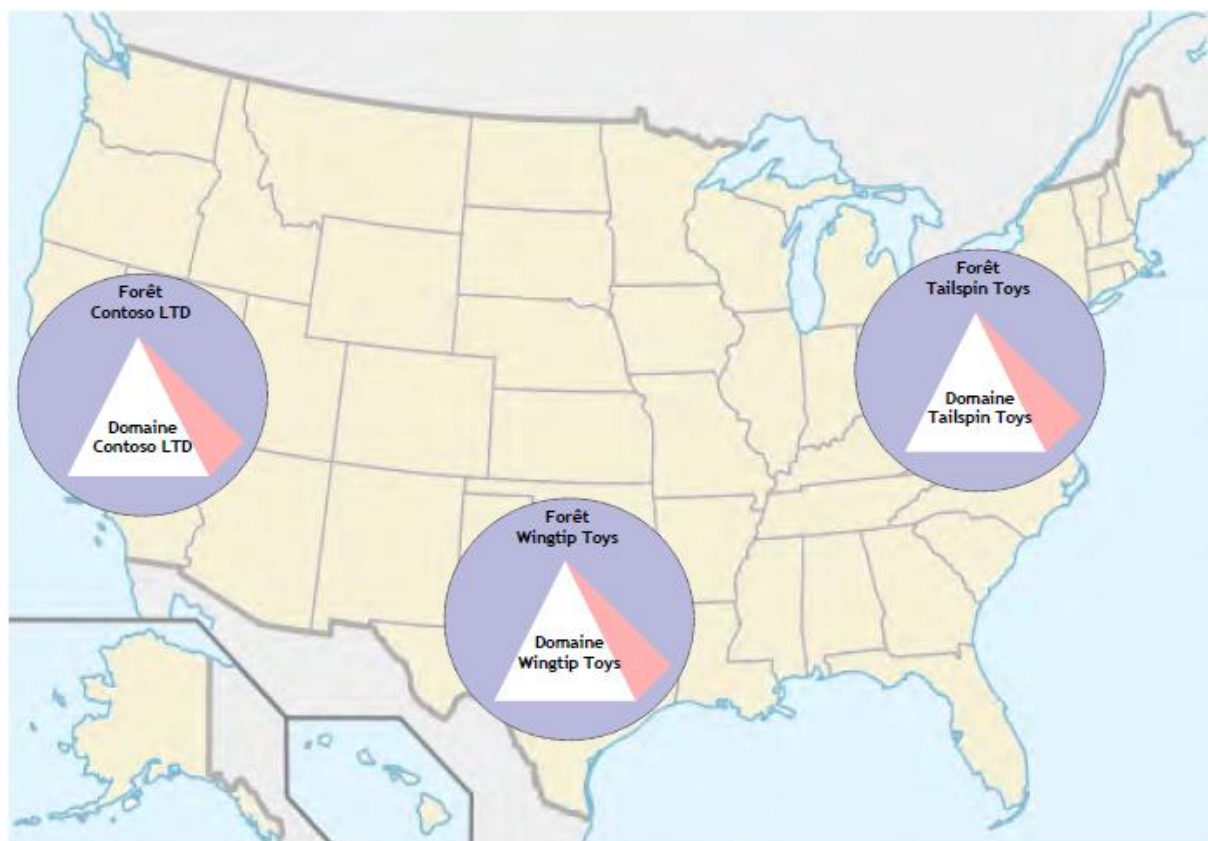
4.2. Infrastructure Active Directory existante

Les trois sociétés composant le groupe Tailspin Toys possède la même architecture Active Directory. C'est-à-dire que chaque entité possède sa propre forêt. Nous avons donc trois forêts distinctes qui ont comme nom de domaine racine :

-  Tailspintoys.lan
-  Contoso.lan
-  Wingtip toys.lan

Il y a à la fois des contrôleurs de domaines sur les sites principaux (siège) et sur les sites de production.

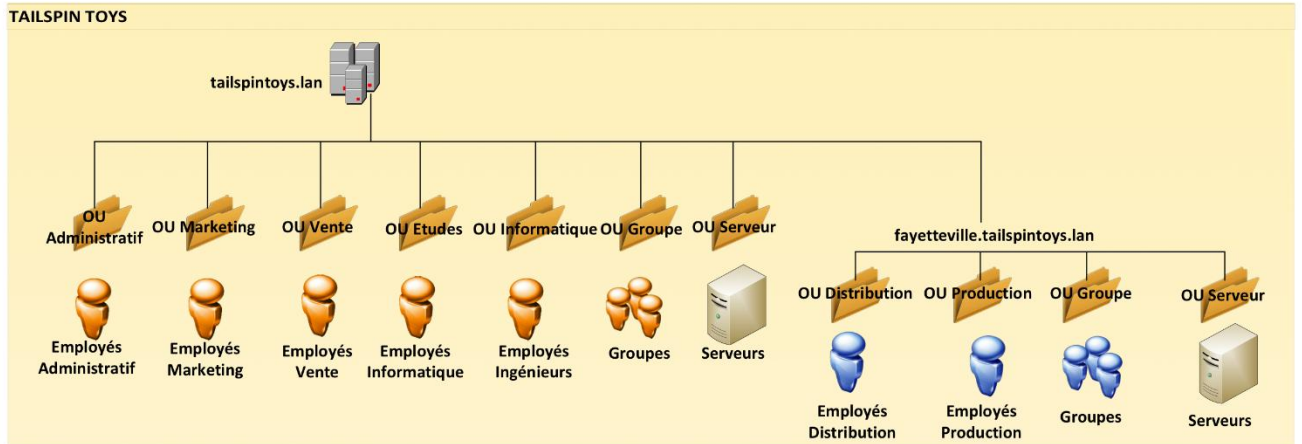
Les informations fournies par la société Tailspin Toys, concernant l'infrastructure Active Directory existante



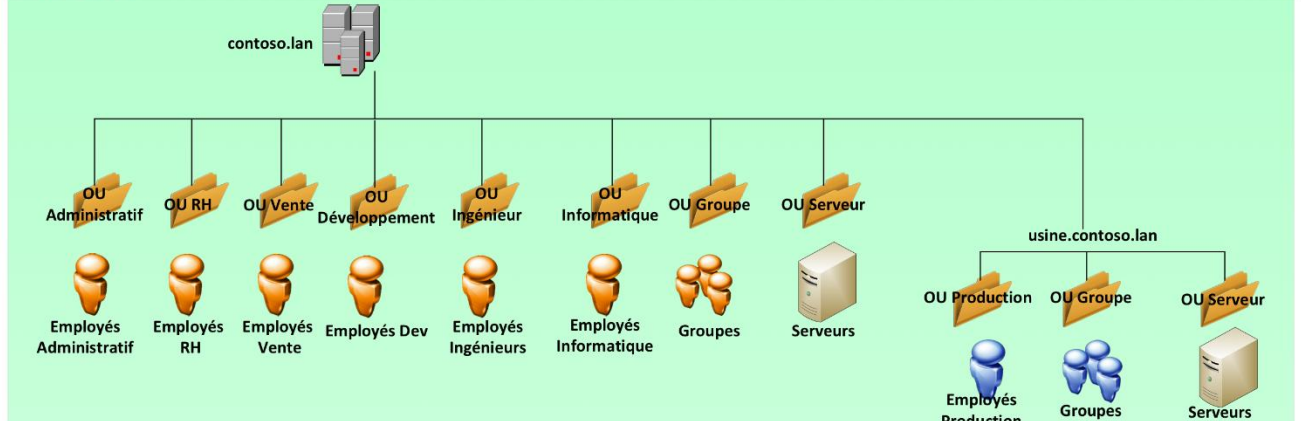
4.3. Relevé des OU

Dans un souci de gestion et d'administration des comptes de l'annuaire active directory de chaque société, des OU (Organizational Unit, ou Unité d'Organisation) ont été mis en place. Cela permet de classer des personnes ou des ressources selon leurs positions géographiques et/ou par rapport à leurs services.

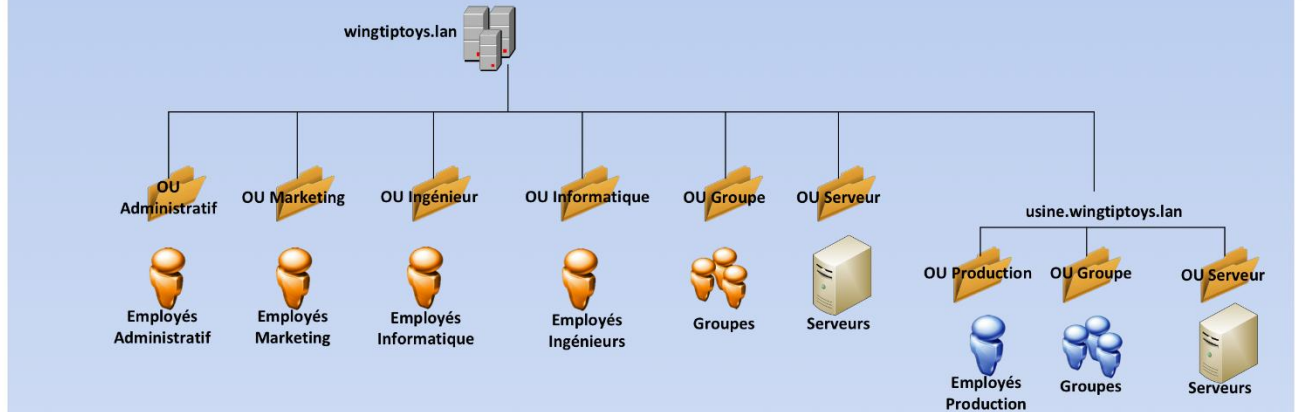
GROUPE TAILSPIN TOYS



CONTOSO, LTD

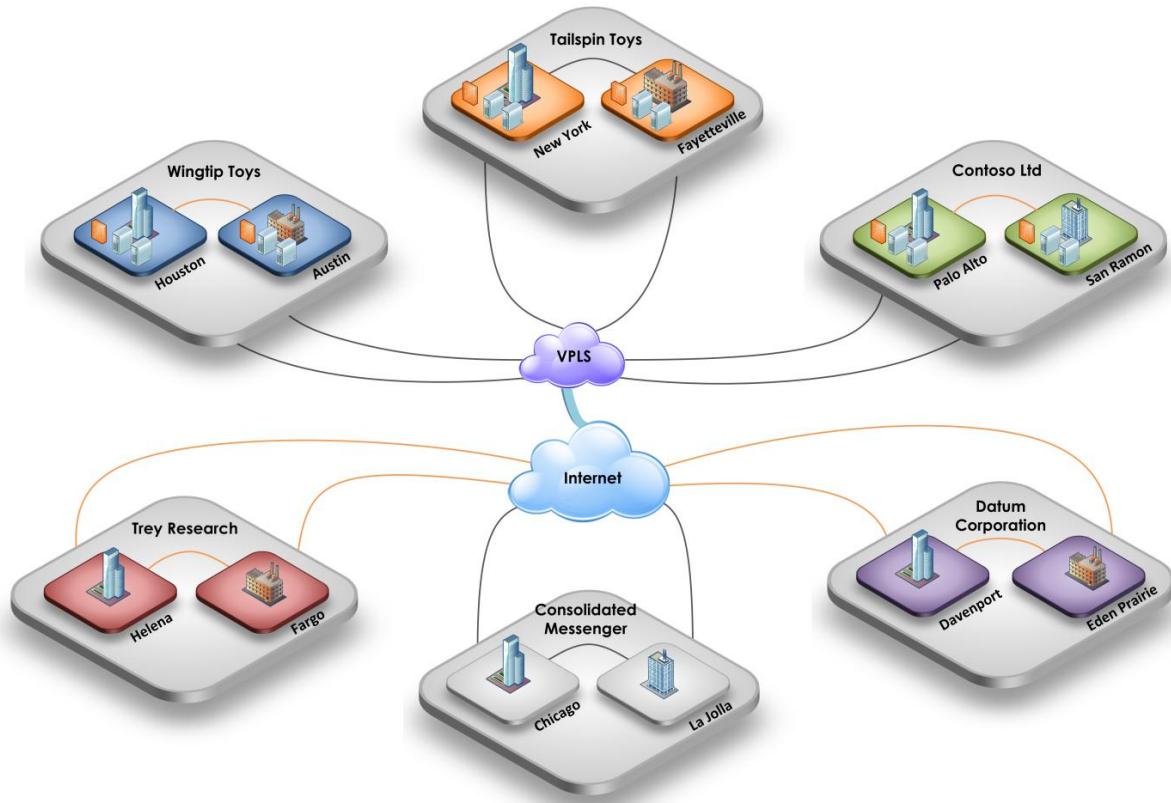




WINGTIP TOYS



5.1. Infrastructure réseau

5.1.1. Schéma du réseau



	Tailspintoys		Contoso		Wingiptoys	
Sites	New York	Fayetteville	Palo Alto	San Ramon	Houston	Austin
	2000	1000	325	50	250	500
	1875	875	430	100	400	200

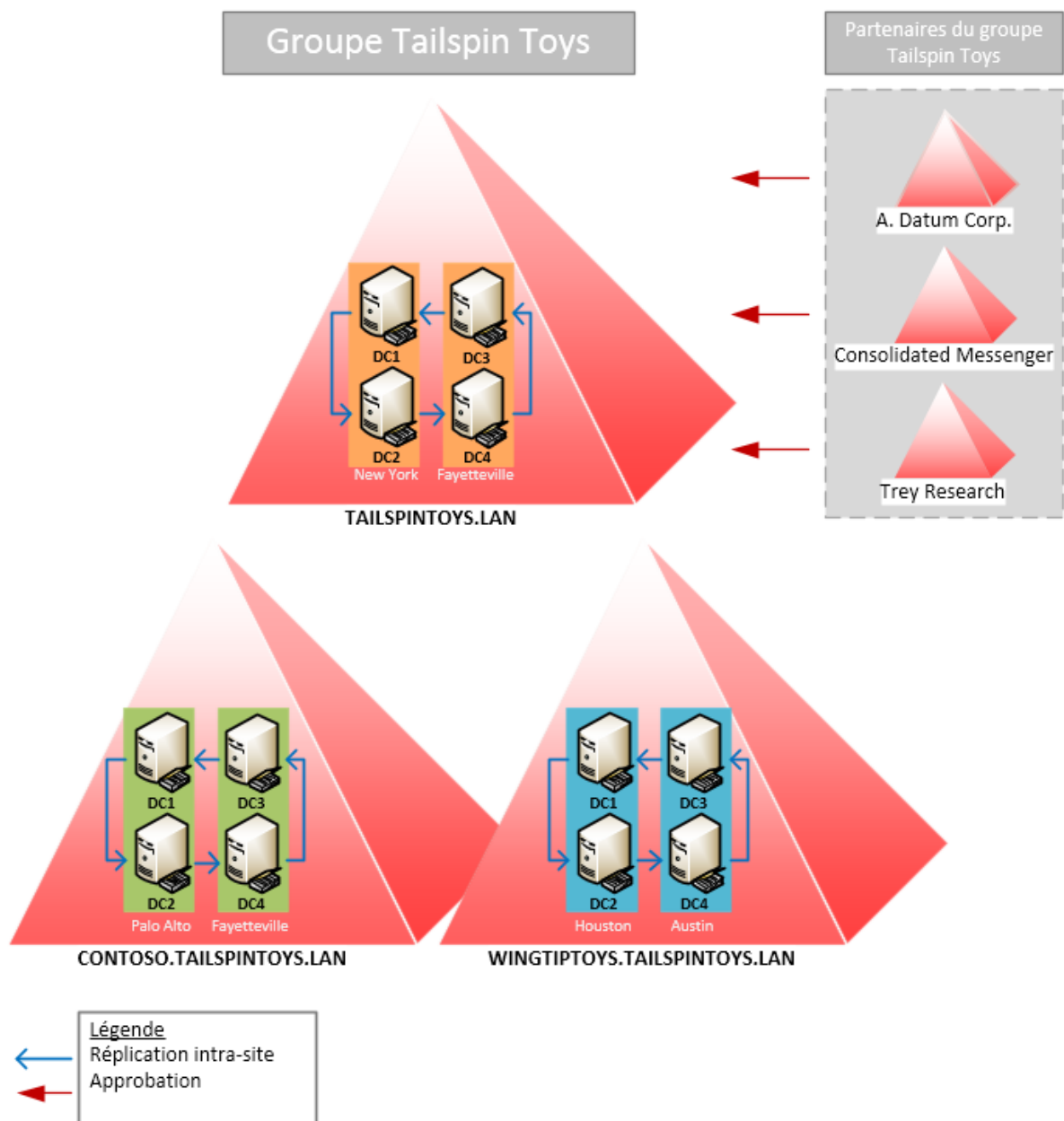
5.1.2. Modifications apportés

Suite au rachat des deux entreprises **Contoso LTD** et **Wingtiptoys**, des modifications au niveau de l'infrastructure réseau ont lieu :

- **L'interconnexion de la maison mère et des deux filiales en VPLS :** C'est une technologie fiable, évolutive et efficace.
- Le remplacement des serveurs physiques hébergeant les contrôleurs de domaines sur les deux filiales par des **ESX**. Ces contrôleurs de domaines seront alors virtualisés (*cette partie sera plus détaillée dans la partie 5.3 Virtualisation*)

5.2. Infrastructure Active Directory proposé

5.2.1. Schéma de l'architecture



5.2.2.Détails sur l'architecture

L'architecture proposé est une forêt unique comprenant le domaine parent ***Tailspintoys.lan*** et de deux domaines enfants ***Contoso.Tailspintoys.lan*** et ***Wingtip toys.Tailspintoys.lan***.

Cela implique :

- Une ***réplication d'objets*** intra-site entre les DC de chaque domaine.
- Une ***réplication de schéma*** inter-site. entre tout les DC de la forêt.

5.2.2.1. Domaine Tailspintoys.lan

Quatre contrôleurs de domaines sont en place actuellement. Aucun rôle supplémentaire ne sera mis en place à l'exception du **catalogue global**.

Le rôle de catalogue global va permettre aux contrôleurs de domaines de contenir une copie de tous les objets Active Directory et permettra donc d'avoir des informations sur les objets des domaines enfants. Ce rôle sera attribué à tout les contrôleurs de domaines.

5.2.2.2. Domaines Contoso.Tailspintoys.lan et Wingtip toys.lan

Huit nouveaux contrôleurs de domaines vont voir le jour en remplacement de ceux déjà existant. Il y en aura quatre dans chaque filiale qui seront répartis entre chaque site. Le fait d'avoir deux contrôleurs de domaines par site va permettre de faire de la répartition de charges et de la tolérance de panne.

Il sera possible de créer un suffixe UPN (sorte d'alias) a chaque domaine de manière à ce qu'ils conservent leurs noms d'origine. Ainsi les utilisateurs ne verront pas différence de nom de domaine et cela ne changera pas la manière dont ils se connectent.

Voici la liste des nouvelles fonctions assurées par les contrôleurs de domaines. Ces derniers se répartissent les rôles FSMO* de domaine et DNS.

- **Contoso.Tailspintoys.Lan**
 - **Palo Alto**
 - DC1 ; DNS, Emulateur PDC,
 - DC2 ; Maitre d'infrastructure
 - **San Ramon**
 - DC3 ; DNS
 - DC4 ; Maitre RID
- **Wingtiptoys.Tailspintoys.lan**
 - **Houston**
 - DC1 ; DNS, Emulateur PDC,
 - DC2 ; Maitre d'infrastructure
 - **Austin**
 - DC3 ; DNS
 - DC4 ; Maitre RID

*Les rôles FSMO sont des rôles de contrôleurs de domaines, ils peuvent agir au niveau du domaine ou au niveau de la forêt. Voici ceux du domaine :

- **Emulateur PDC** ; Gère les changements de mot de passe et maitre du temps
- **Maitre d'infrastructure** ; Synchronise les changements inter-domaines
- **Maitre RID** ; Fournit des tranches d'identifiants uniques aux autres contrôleurs de domaine.

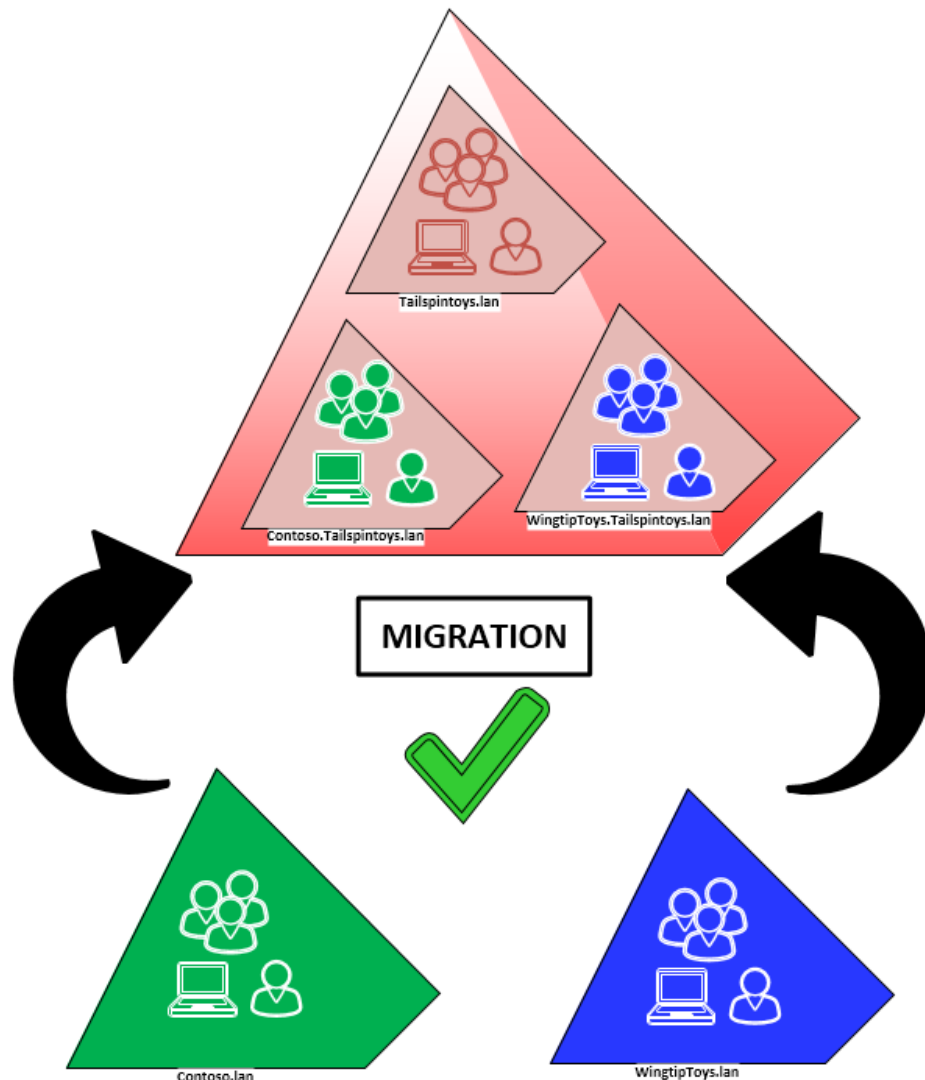
5.2.2.3. Partenaires du groupe

Etant donné que les entreprises partenaires **A. Datum Corporation**, **Consolidated Messenger** et **Trey Research** ont besoin d'avoir accès à certaines ressources partagées de **Tailspintoys.lan**, une relation d'approbation entre domaine sera mis en place.

5.2.3.Scénario de migration

Dans le cadre de la nouvelle solution proposée, il est nécessaire de repasser par la restructuration de votre environnement afin d'optimiser l'organisation des éléments au sein de la structure Active Directory.

Dans notre cas, la restructuration implique de migrer des ressources entre les domaines Active Directory au sein de forêts différentes réuni en 3 domaines enfants de la forêt Tailspin Toy.



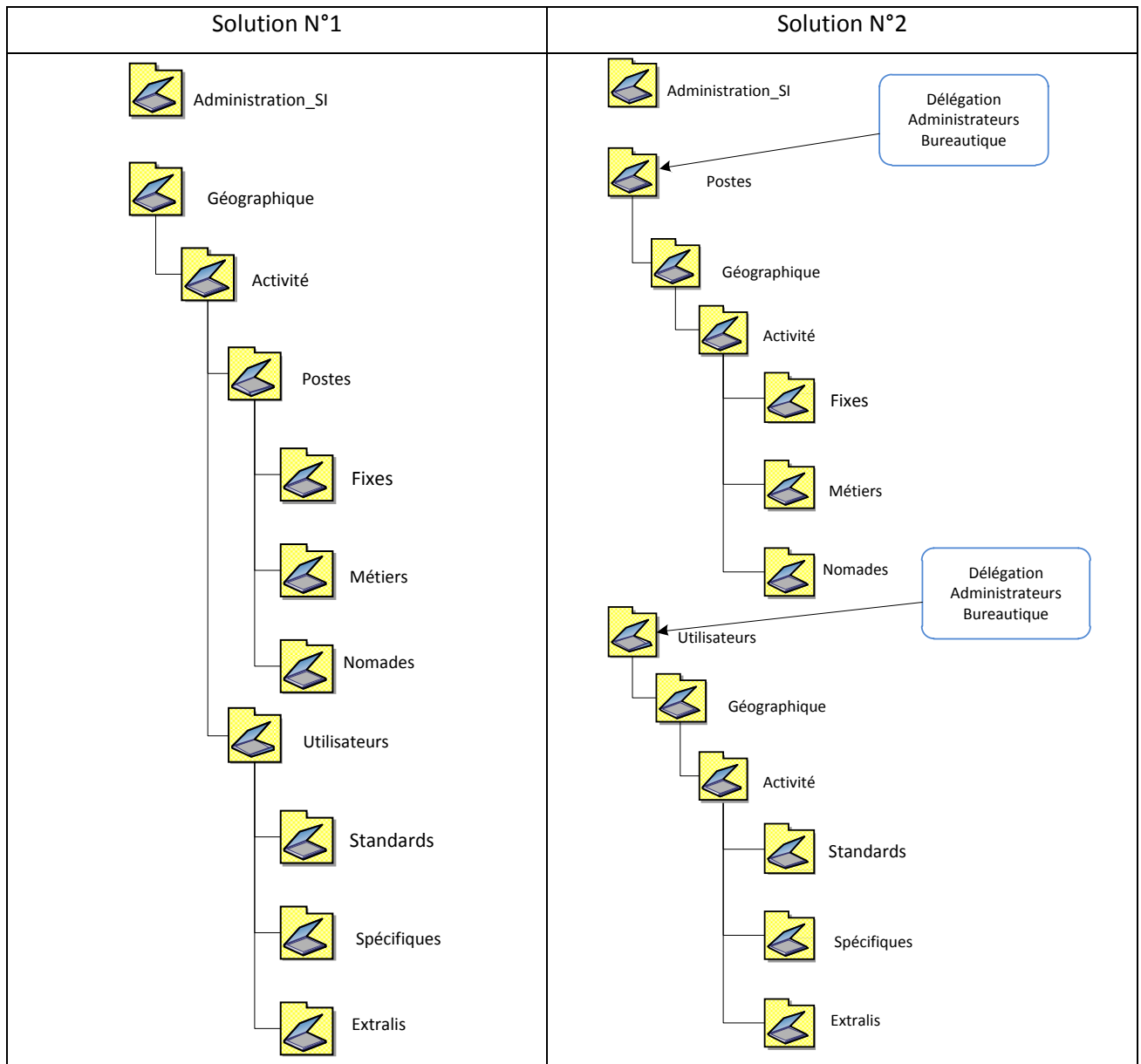
Nous utiliserons l'outil de migration Active Directory, ADMT, afin d'effectuer les migrations d'objets et le maintien d'appartenance aux groupes lors du processus proposée de migration inter-forêts.

5.2.4.Organisation des nouvelles OU

Les 2 solutions d'arborescence des OU répondent à plusieurs besoins :

- Recherche rapide des comptes ordinateurs et utilisateurs par les équipes de support
- Application de GPO et de script
- Facilité de délégation d'administration

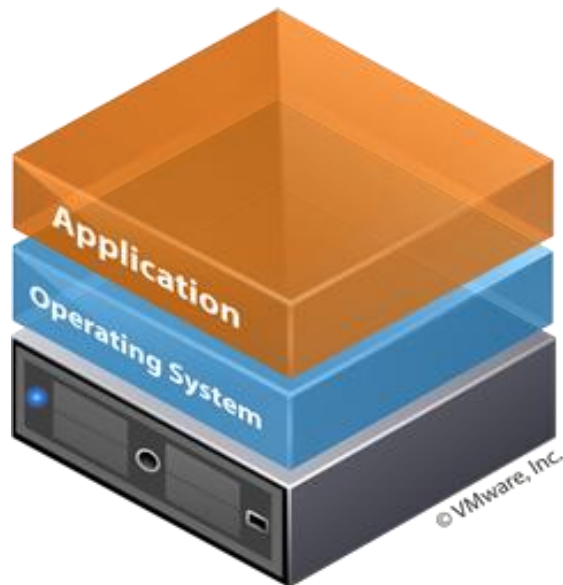
Dans l'optique de facilité la délégation du travail d'administrateur bureautique, nous proposons d'inverser les niveaux postes/utilisateurs avec le niveau géographique, la solution n°2 est préconisée.



5.3. Virtualisation

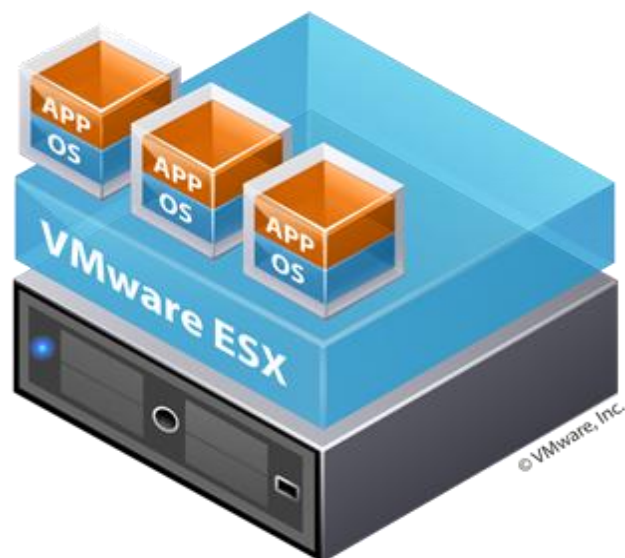
5.3.1.Présentation

La majorité des ordinateurs actuels (x86) ont été pensés pour exécuter un seul système d'exploitation et une seule application, résultat, la plupart des machines sont sous-utilisées.



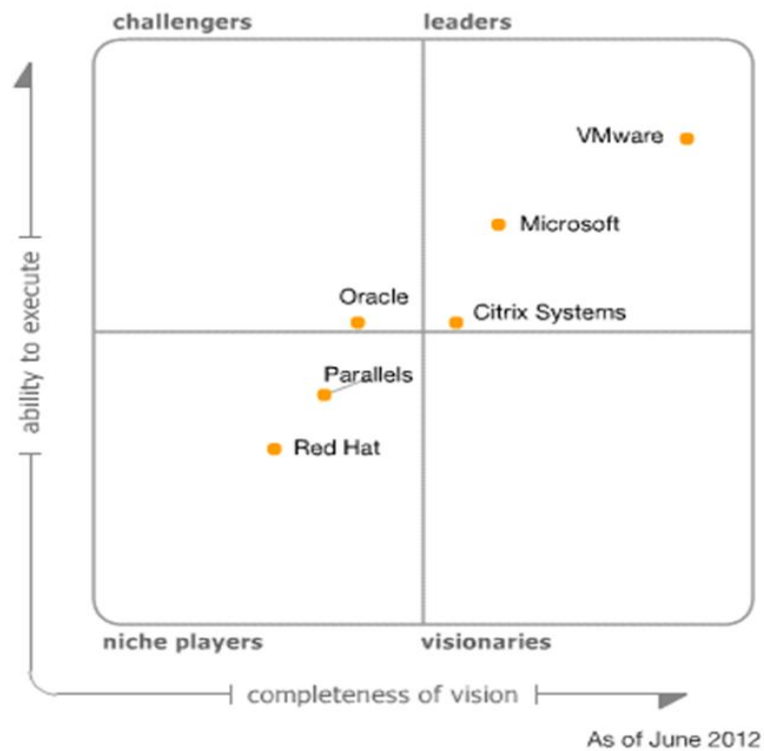
La virtualisation consiste à faire fonctionner sur un seul ordinateur plusieurs systèmes d'exploitation comme s'ils fonctionnaient sur des ordinateurs distincts. On appelle serveur privé virtuel (Virtual Private Server ou VPS) ou encore environnement virtuel (Virtual Environnement ou VE) ces ordinateurs virtuels.

De la même façon que l'on fait fonctionner plusieurs programmes sur un même OS (multitâches) nous savons faire fonctionner plusieurs OS sur un même hardware.





VMware est une société informatique américaine fondée en 1998, filiale d'EMC Corporation depuis 2004, elle propose plusieurs produits propriétaires liés à la virtualisation d'architectures x86. Aujourd'hui VMware est le leader incontesté de la virtualisation et propose une solution beaucoup plus complète que ces principaux concurrents, c'est pourquoi nous préconisons pour Tailspin Toys d'utiliser les solutions VMware.



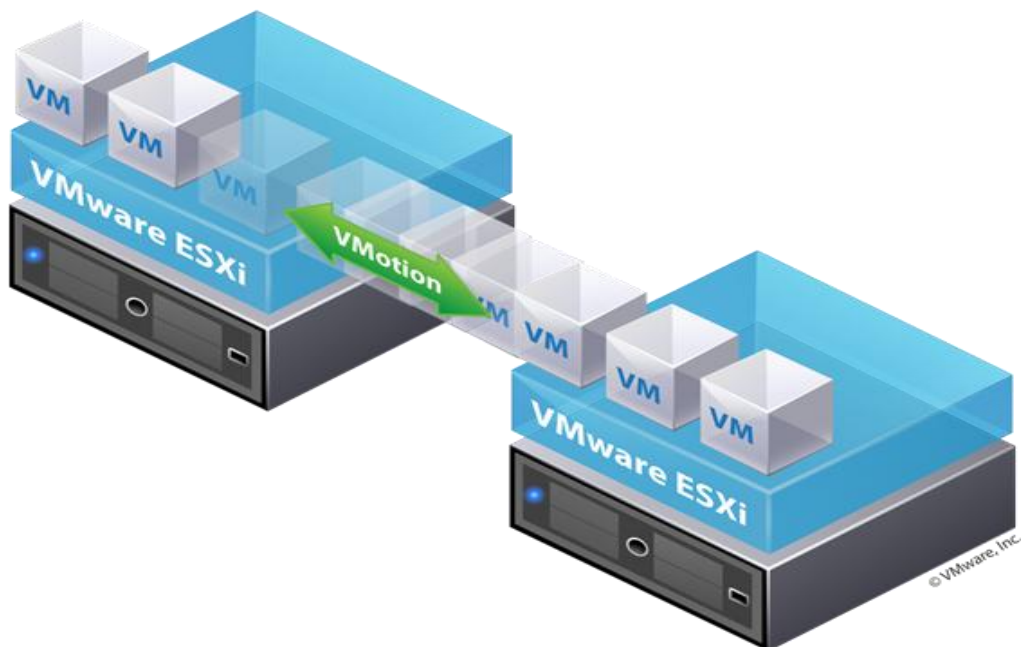
5.3.2. Qu'est-ce que la virtualisation

La virtualisation permettra à Tailspin Toys:

- L'utilisation optimale des ressources de son parc de machines (répartition des machines virtuelles sur les machines physiques en fonction des charges respectives).
- Différentes machines virtuelles sont capables d'exécuter divers systèmes d'exploitation et plusieurs applications sur le même ordinateur physique.
- L'installation, déploiement et migration facile des machines virtuelles d'une machine physique à une autre.
- De diminuer les dépenses d'investissement.
- D'économie sur le matériel par mutualisation (consommation électrique, entretien physique, surveillance, support, compatibilité matérielle, etc.)
- La sécurisation et/ou l'isolation d'un réseau.
- L'allocation dynamique de la puissance de calcul en fonction des besoins de chaque application à un instant donné.

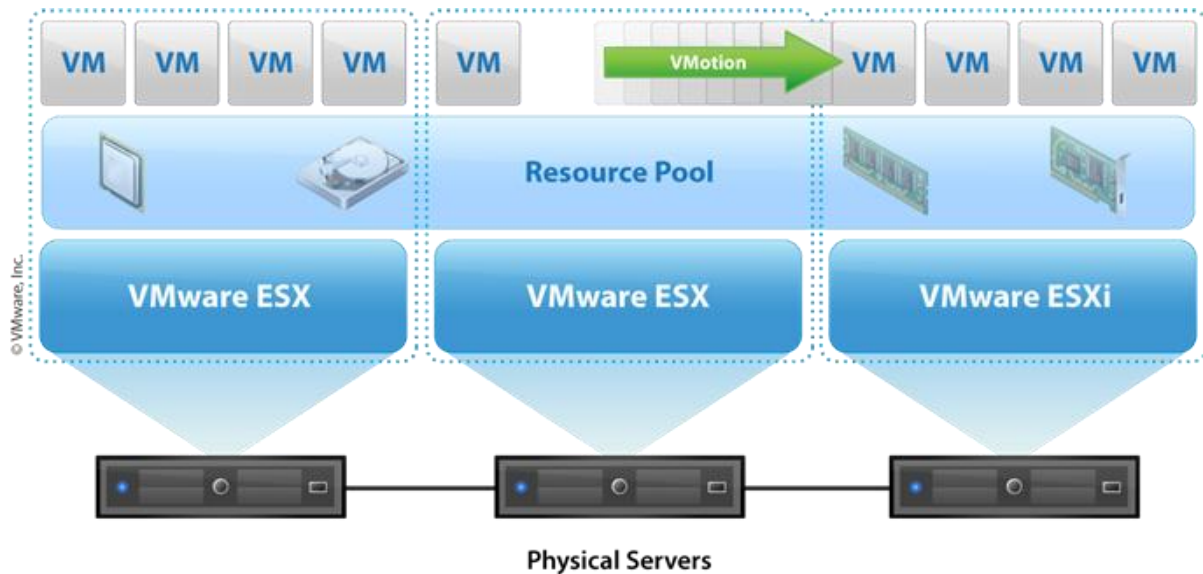
En outre de tous ses avantages, la virtualisation va apporter à Tailspin Toys une multitude de service qui va à la fois augmenter le rendement de ces informaticiens tout en diminuant son OPEX :

Le Vmotion



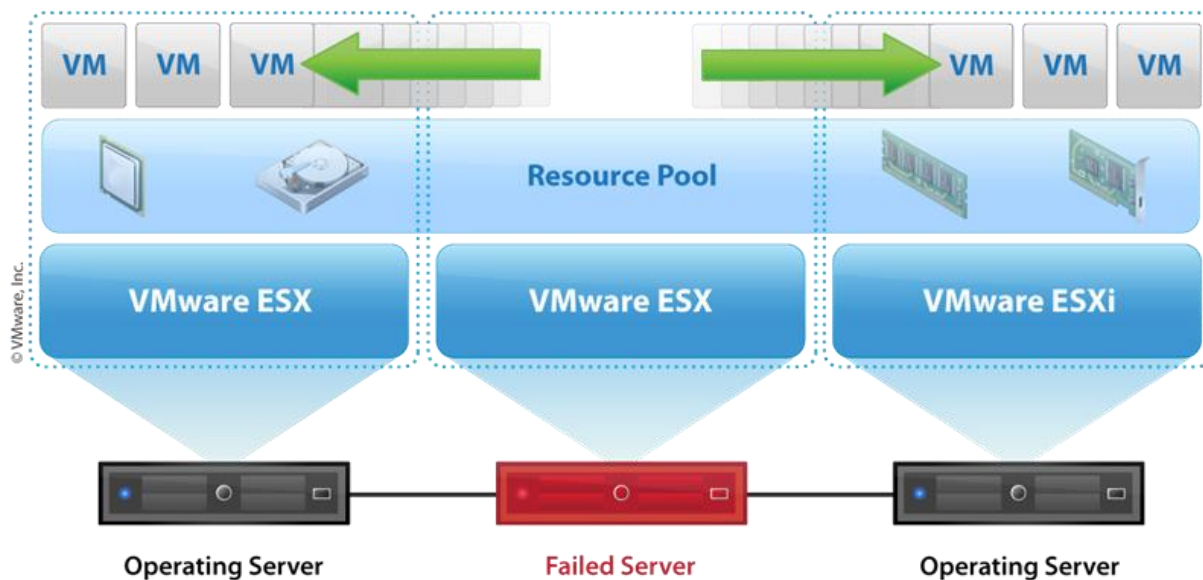
Le Vmotion permet de déplacer en direct une machines virtuelles en service depuis un serveur physique vers un autre serveur sans période d'interruption avec une disponibilité de service permanente et une intégrité de transaction complète.

Le DRS (Distributed Ressources Scheduler)



Ce Service va permettre équilibrer la capacité informatique dynamiquement dans les Cluster de ressources matérielles pour les machines virtuelles. Cette fonction comporte des possibilités de gestion d'alimentation distribuée (DPM) permettant au centre de données de réduire significativement sa consommation d'énergie par exemple éteindre un des ESX qui contiens des servers peu ou pas utiliser pendant la nuit.

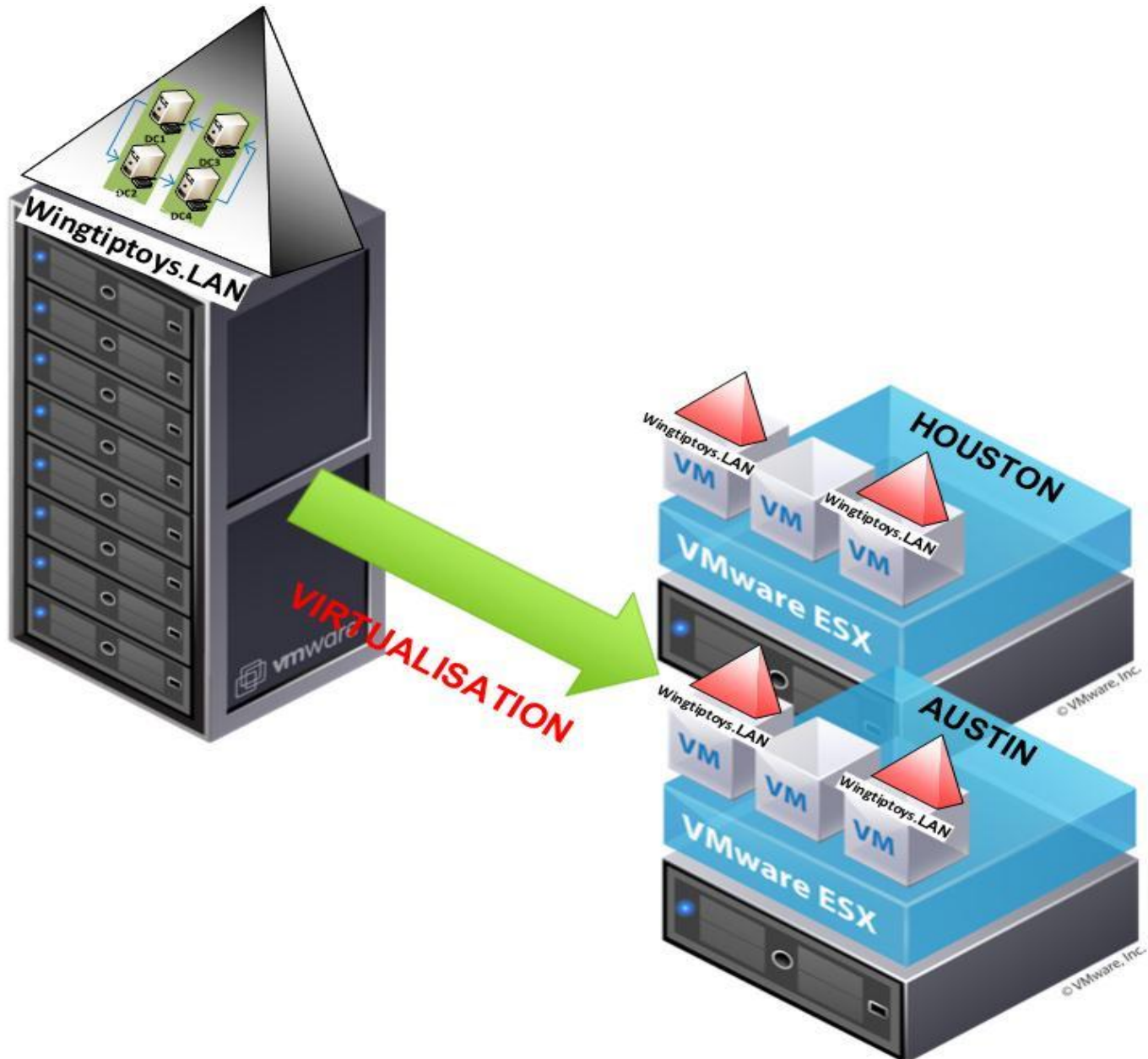
Le HA (High Availability)



C'est une fonction qui offre une haute disponibilité aux machines virtuelles. En cas de panne du serveur, les machines virtuelles affectées sont redémarrées sur d'autres serveurs de production disposant de surcroît de capacité.

5.3.3. Comment allons-nous procéder pour virtualiser l'AD de Tailspin Toys

Nous préconisons pour Tailspin Toys de virtualiser seulement les serveurs des entreprises qu'elle vient d'acquérir Contoso LTD et Wingtip Toys, la procédure sera la même pour les deux entités :



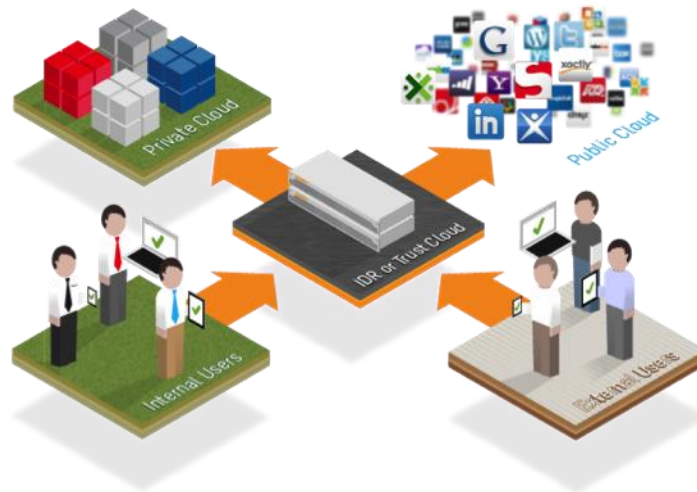
Grace à cette procédure de virtualisation Tailspin Toys :

- Pourra économiser quatre serveurs, 2 à Contoso LTD et 2 à Wingtip Toys. Elle pourra par la suite soit les retirés et faire donc des économies d'énergie et de maintenance ou bien les réutiliser afin d'augmenter sa puissance de calculs (rajout de nouvelles applications).

Elle facilitera la gestion de ces serveurs et aura un gain de temps pour les opérations de maintenance (déplacer une machine d'un serveur vers un autre).

5.4. Cloud

5.4.1. Qu'est-ce que le Cloud ?



Chacun utilise des applications sur Internet et fait donc du cloud computing: jeux, service de traduction, webmail, etc.

Mais l'intérêt primordial du cloud computing est pour les entreprises qui ne sont plus limitées à des parcs informatiques figés et à des palettes d'applications fixes.

Si l'entreprise a besoin d'une capacité machine plus élevée pendant un certain temps, elle la loue pour la durée nécessaire, "à la demande", et l'exploite immédiatement. Pas de choix de matériel à effectuer, pas d'achat, pas d'installation, pas de configuration, pas d'administration.

Donc:

- Rapidité extrême
- Simplicité
- Flexibilité
- Economie d'investissement et probablement de coûts
- Plus de machine inexploitée ou sous-exploitée une fois le besoin échu
- Idem pour une capacité de stockage requise temporairement

Les avantages persistent même si l'utilisation est permanente :

- Dans le cas du matériel, parce qu'on peut moduler les ressources de calcul et de stockage en fonction des besoins et, surtout, qu'on peut externaliser le travail nécessaire pour gérer cette plate-forme.
- Dans le cas des applications, parce qu'on dispose constamment des dernières versions des logiciels et qu'on ne doit pas se soucier d'administrer les applications concernées.

5.4.2. Solution de Cloud pour l'Active Directory



Windows Azure est le service d'intégration d'Active Directory dans le Cloud, communément appelé WAAD.

Le service d'annuaire Active Directory répertorie les éléments d'un réseau comme les comptes utilisateurs, les serveurs, les postes de travail, les dossiers partagés, les imprimantes, les bases de données, etc. Il fournit des services centralisés d'identification et d'authentification à un réseau d'ordinateurs sous Windows.

Windows Azure Active Directory (WAAD) utilise les capacités d'entreprise d'Active Directory pour Windows Server, afin de permettre de placer facilement les applications dans le Cloud. La meilleure façon de décrire WAAD est que Microsoft permet à Active Directory d'une entreprise de fonctionner sur le Cloud, tout comme sur Windows Server en local.

Le service Cloud Active Directory repose sur des fonctionnalités d'identité et d'accès qui ont été redéfinies pour être utilisées dans les écosystèmes interconnectés actuels qui sont de plus en plus hétérogènes. WAAD a donc été élargi pour supporter les terminaux mobiles comme l'iPhone, les plateformes Cloud comme AWS et les technologies comme Java.

Conçu pour la haute disponibilité à l'échelle d'internet, WAAD est déjà utilisé pour la gestion de l'identité pour Office 365 et Windows Intune.

Le service de contrôle d'accès (ACS) de WAAD permettra d'utiliser un seul portail pour gérer tous les utilisateurs et groupes à travers les applications Cloud. ACS est compatible avec plusieurs plateformes Web modernes, y compris .NET, PHP, Python, Java et Ruby.

Cette configuration de Cloud est une solution qui permettrait à Tailspin Toys de répondre à des problématiques de PCA/PRA, s'il arrivait un incident ou une catastrophe climatique qui détruirait les sites de Tailspin Toys, son annuaire sera toujours disponible.



Mais cette solution à un coût élevé, Tailspin Toys aura besoin de louer les services d'un Cloud à long terme.

Il est peu probable que les annuaires du même domaine, qui se situe sur différents sites, soient détruits au même moment.

C'est pourquoi nous ne préconisons pas à Tailspin Toys de retenir la solution du Cloud néanmoins si il le souhaite nous pourrions répondre à sa demande et lui réaliser mettre en place son annuaire dans le Cloud.

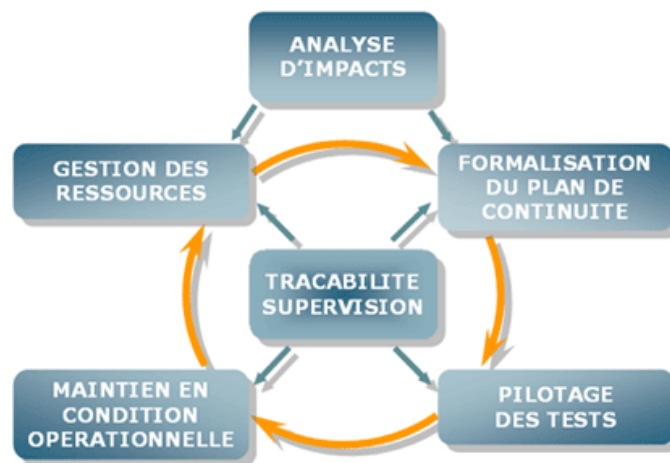
5.5. PCA / PRA

Le service d'annuaire Active Directory est un service critique qui doit assurer un haut niveau de disponibilité pour minimiser l'impact sur les autres services de l'entreprise. Pour atteindre ce résultat, un plan de continuité d'activité et un plan de reprise d'activité doivent être mis en place.

La mise en place d'une solution PCA/PRA nécessite en amont de procéder à :

- **Une analyse des risques** ; Qu'ils soient humains ou d'origine naturelle et évaluer le taux de probabilité.
- **Une analyse d'impact** ; Evalue l'impact d'un risque et détermine à partir de quand cet impact est intolérable et met en danger la survie de l'entreprise. Les types d'impact peuvent être humains, financiers, légaux, etc.

5.5.1. Plan de continuité d'activité



Le plan de continuité d'activité (PCA) est un ensemble de mesure préventive qui va permettre de continuer l'activité sans subir d'interruption de service. L'élaboration de ce plan nécessite la mise en place de certains points :

- **Elaborer un plan de continuité** : Afin de définir les responsables et les mesures qu'il y aura à prendre.
- **Mettre en place une redondance des contrôleurs de domaines** ; Lorsqu'un contrôleur de domaine n'est plus en état de fonctionner, un autre prendra le relais. Cela implique de ne pas les mettre dans les mêmes salles serveurs et relativement éloigné. Des mesures peuvent être prise pour rendre les serveurs moins vulnérable ; comme le doublement d'aliment des baies de serveurs.
- **La répartition de charges (Load Balancing)** ; Les requêtes sont répartis entre chaque serveur afin de ne pas les surcharger. On peut aussi considérer les technologies comme RAID qui permettent une redondance de disques par exemple.
- **La mise en place d'une équipe de maintien en condition opérationnel** ; Afin de veiller à ce que l'infrastructure informatique soit constamment en état de fonctionnement optimal. Lorsqu'un problème intervient sur un équipement (exemple ; un des contrôleurs de domaines), un ticket de maintenance est émis et un administrateur sera en charge de le résoudre dans un temps imparti défini à l'avance (SLA).

- **La mise en place d'un système de supervision** ; Très utile afin de surveiller l'état des équipements. En cas de problème, une alerte remonte à l'équipe MCO (Maintenance en condition opérationnel), et cette dernière peut rapidement prendre en charge l'incident.
- **La rédaction de procédure** : Ces procédures permettront de savoir quoi faire en cas de crise.
- **L'élaboration de tests de manière régulière** ; Des simulations de crises doivent être effectuées afin de permettre à l'entreprise d'être préparée. Cela permet aussi de sensibiliser les utilisateurs aux risques d'une crise et de tester les procédures.

5.5.2. Plan de reprise d'activité



Un PRA va permettre d'assurer la reconstruction de l'infrastructure informatique et la remise en route des applications nécessaires à l'activité de l'entreprise dans un délai prédéfini. Le basculement de l'activité vers le plan de reprise d'activité se fera lors d'un événement majeur qui paralyserait l'activité d'un site par exemple.

La mise en place de ce PRA nécessite la **mise en place de sauvegarde des contrôleurs de domaines**; expliqué dans la partie suivante

Il faut au préalable :

- Fixer une durée maximale d'interruption de service (temps entre le moment de l'interruption de service et la reprise de l'activité)
- Fixer la perte de données admissible (jusqu'où remonte la dernière sauvegarde des données récupérées)

Dans le cas où tout le site est paralysé, diverses solutions sont possibles :

- **L'utilisation d'un site froid** : site de secours qui peut avoir une autre utilisation en temps normal ou sont stockés des serveurs et du matériel non installés et non connectés
- **L'utilisation d'un site tiède** : site de secours intermédiaire contenant des serveurs et des machines connectés et installés (mais non forcément à jour) éteints et prêts à être allumés.
- **L'utilisation d'un site chaud** : site de secours contenant des serveurs et des machines installés connectés et à jour, allumés et prêts à fonctionner. La mise en place d'un tel site revient à faire une redondance totale du parc informatique et est très onéreuse.

Le basculement vers le PRA ne serait pas possible sans une sauvegarde efficace.

5.6. Sauvegarde



5.6.1. Préparation de la sauvegarde

Pour garantir le basculement vers le Plan de Reprise d'Activité en cas de crise ou tout simplement en cas de perte de données, la sauvegarde est un élément clés. Microsoft met à disposition sur *Windows Server* un outil spécialement conçus pour cette tâche; *Utilitaire de sauvegarde*. Ce dernier va permettre de prendre deux types de clichés (sorte de photographie d'un système d'exploitation à un instant T) :

- **Clichés du service d'annuaire;** Essentiel pour s'assurer de récupérer les données de ce dernier, dans l'éventualité d'un événement provoquant la corruption ou la destruction de l'installation Active Directory.
- **Clichés du système;** Ont pour utilités de pouvoir restaurer le système sur laquelle est installé le contrôleur de domaine en cas de défaillance du système de stockage ou autre problème pouvant impacter le fonctionnement de l'annuaire.

La sauvegarde s'effectuera de manière quotidienne sur chaque contrôleur de domaine, pendant la nuit et de manière transparente pour l'utilisateur.



5.6.2. Etape de sauvegarde

La sauvegarde s'effectuera en deux étapes :

- **L'enregistrement des clichés** sur un **serveur de sauvegarde** ; Ce dernier va conserver pendant une durée de un mois les sauvegardes sur disques durs.
- **L'archivage sur bandes de stockage;** Chaque mois, les clichés contenu sur le serveur de sauvegarde seront archivés pendant un laps de temps défini (pouvant aller de 6 mois à quelques années). Un lecteur de bande est nécessaire et se chargera d'écrire les informations sur bandes. Ces dernières seront ensuite stockées en lieu sûr.

5.6.3.Support de sauvegarde




Voici les solutions de supports proposés pour la sauvegarde :

	Serveur de sauvegarde	Lecteur de bande
Modèle	HP Proliant DL360 Gen7 	HP MSL2024 1-lto-6 
Capacité	8 disques SATA	24 bandes
Stockage	8x1 Téra Octet en RAID 5 La capacité de stockage n'a pas besoin d'être excessive dans le sens où les données sont archivées par la suite.	48 x 800 Giga Octet En fonction du volume des sauvegardes, on utilisera une ou deux bandes chaque mois.

6. PLANNIFICATION DU PROJET

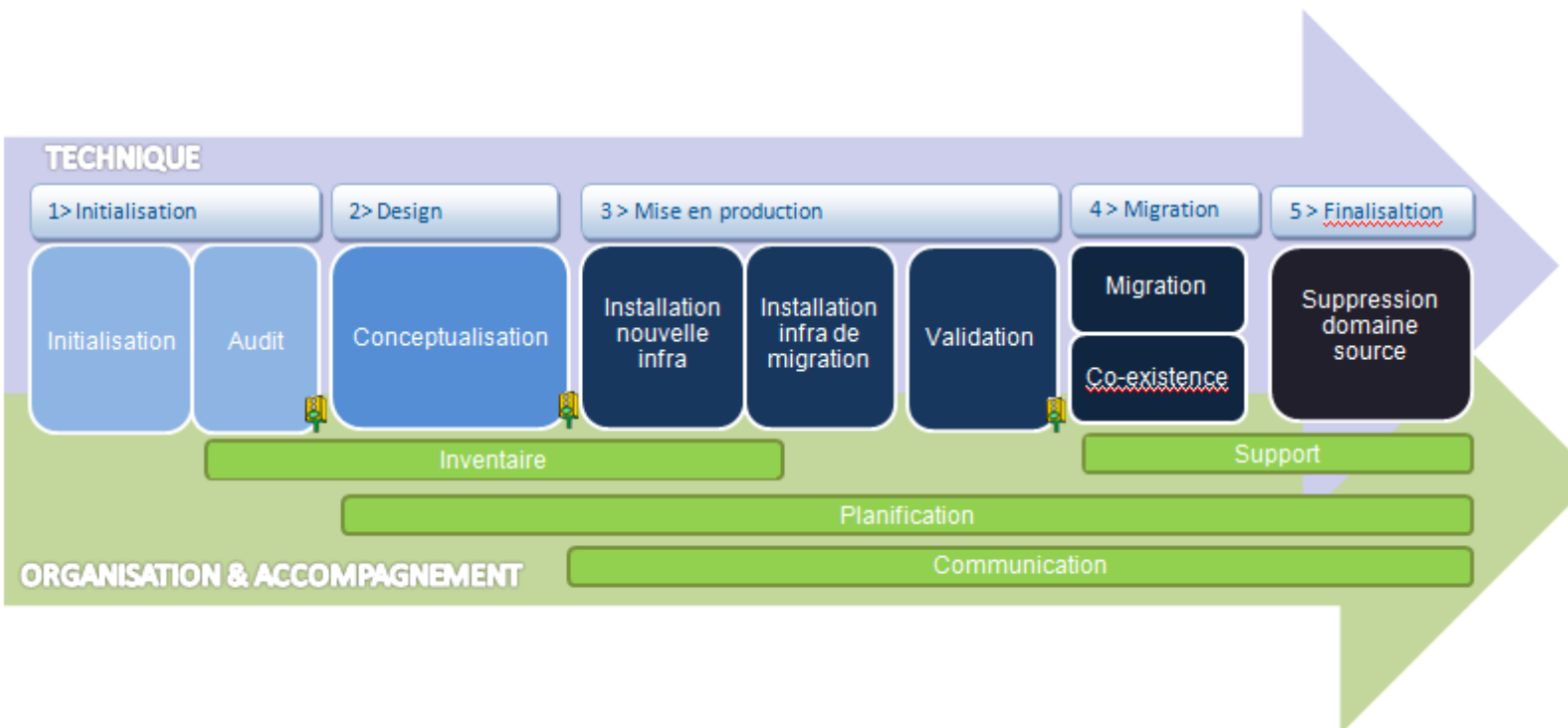
6.1.1. Vision macroscopique du projet

Les grandes phases projet :

-  Phase 1 « Initialisation » : étude, cadrage et design
-  Phase 2 « Réalisation » : implémentation de la nouvelle infrastructure, migrations des objets
-  Phase 3 « Finalisation » : suppression des domaines sources

6.1.2. Vision détaillée du projet

Chacune de 5 phases principales exposées ci-dessus comporte plusieurs étapes qui pourront être développées dans un plan d'actions détaillé ultérieur.



Cinq temps clés sont identifiés dans le projet de refonte de l'infrastructure :



7. EVALUATION FINANCIERE

En tant qu'intégrateur, nous ne sommes pas agréé pour vendre les licences ou pour négocier des prix sur le matériel informatique. Ce sont des prérequis qu'il faudra revoir plus en détails suite à un audit.

Description des produits et services	JOUR	Coût unitaire	Coût TOTAL
Etude de cadrage	10	650 €	6 500 €
Audit des contraintes Active Directory et applicatives	2		
Identification des contraintes auprès des équipes informatique des 2 filiales de Tailspin Toys	1		
Livrable : Compte rendu de l'audit	1		
Définition de la cible – initialisation conception	8		
Revue et validation de l'architecture cible	1		
Définition de la migration	3		
Définition des planifications des migrations	2		
Livrable : Initiation Dossier d'architecture	2		
Conception	6	650 €	3 900 €
Rédaction du plan d'action détaillé	2		
Définition du plan d'action détaillé	1		
Livrable : Plan d'action détaillé	1		
Rédaction des procédures détaillées	2		
Définition des procédures détaillées	1		
Livrable : Cahier de procédures	1		
Rédaction du cahier de recette	2		
Rédaction du cahier de recette	2		
Livrable : Cahier de recette			
Réalisation	13	530 €	6 890 €
Assistance à la mise en œuvre de la nouvelle infra	5		
Installation des ESX et configuration des nouveaux DC	5		
Installation infrastructure de migration	1		
Serveur ADMT et service	1		
Migrations pilote (50 postes/groupes/utilisateurs et 2 serveurs)	7		
Test de migration	6		
Livrable : Cahier de recette	1		
Assistance technique post migration pilote	40	650 €	26 000 €
Assistance à la demande pour migration réelle	40		
Gestion de projet	12	565 €	6 780 €
Gestion de projet	12		
TOTAL PROJET	78		50 070 €

8. CONCLUSION

Ce document résume les points techniques à aborder afin de répondre aux mieux à vos besoins. La conception d'une architecture Active Directory est une tâche critique et essentielle au sein d'un système d'information. IZI'T espère avoir apporté une réponse à la hauteur de vos attentes, et qui répondra à votre problématique au travers de ce document.

Aussi, il est important pour IZI'T de prévoir des échanges afin de discuter des aspects techniques, des coûts et de la planification. Ceci, dans le but de pouvoir fournir rapidement un document d'architecture technique reprenant les spécifications techniques ainsi qu'un plan de migration.

La réponse d'appel d'offres proposée et la prestation, si ce dossier est retenue, s'intègre dans un mode de travail collaboratif impliquant une disponibilité d'un ou plusieurs membres de l'équipe projet, pendant la durée du déploiement.

