Concevoir un Plan de Continuité d'Activité (PCA) pour les applications critiques et/ou un Plan de Reprise d'Activité (PRA) structuré permettant de répondre à un maximum de scénarios d'incidents

Thomas Tellier

CONSERVATOIRE NATIONAL DES ARTS ET METIERS

Centre Régional : Rhône-Alpes

MÉMOIRE

Présenté en vue d'obtenir

Le **DIPLÔME D'INGÉNIEUR C.N.A.M**

Dans la spécialité

INFORMATIQUE

Par

Thomas TELLIER

Sujet : Concevoir un **P**lan de **C**ontinuité d'**A**ctivité (PCA) pour les applications critiques et/ou un Plan de Reprise d'Activité (PRA) structuré permettant de répondre à un maximum de scénarios d'incidents.

Soutenu le 24/05/2016

Jury

Président : M. Christophe PICOULEAU

Membres : M. Bertrand DAVID

M. Claude GENIER

M. Claudio SIMONE

Remerciements

Je souhaiterai avant tout chose remercier l'ensemble des agents de direction du groupe Veltigroup SA et des sociétés qui le composent qui m'ont permis de travailler sur ce sujet et qui m'ont accordé leur totale confiance.

Je tiens plus particulièrement à remercier M. Claudio Simone, responsable du service informatique du groupe Veltigroup SA, pour l'aide qu'il m'a apporté tout au long de ce travail (autant technique que logistique) et pour sa collaboration lors des multiples réunions et explications que nous avons dû mener.

Je présente également tous mes remerciements aux responsables de chaque service pour leur aide apportée quant à la formalisation de leur processus métier et à la description de leurs activités.

Enfin, je tiens à remercier l'administration du CNAM qui m'a autorisé à travailler sur ce projet qui, au-delà du cadre de ma formation à un diplôme d'ingénieur, m'aura permis d'élargir et d'approfondir mes connaissances.

Avant-Propos

Ce mémoire est le résultat d'un projet d'une durée de 8 mois au sein du service informatique du groupe de services IT, Veltigroup SA. Groupe suisse implanté en Romandie et en Suisse alémanique.

Il a été rédigé en vue de l'obtention d'un diplôme d'ingénieur informatique au sein du CNAM et entre dans la cadre du développement et de l'évolution du groupe.

La réalisation de ce projet a été complexe de par le nombre d'acteurs qui y ont joué un rôle et par la nécessité d'avoir une connaissance transverse de l'ensemble de l'organisation du groupe. La phase d'analyse et d'étude fonctionnelle a donc été décisive quant à ma compréhension générale du fonctionnement d'une société de service informatique.

J'ai réellement apprécié de pouvoir travailler avec l'ensemble des équipes techniques, commerciales et supports.

Le fait que plusieurs incidents se soient déroulés pendant la durée du projet : début d'incendie, coupure des climatisations et arrêt des systèmes informatiques, montre à quel point il est nécessaire de disposer d'un plan de continuité d'activité.

TABLE DES MATIÈRES

GLOSSAIRE

PCA	Plan de Continuité d'Activité	Un plan mis en œuvre au sein d'une société et qui a pour objectif de minimiser les impacts d'une crise ou d'une catastrophe.
PRA/DRP	Plan de Reprise d'Activité Data Recovery Plan	Plan qui permet une reprise ordonnée des activités d'une entreprise suite à une crise majeure.
Outsourcing	Externalisation	L'outsourcing peut se définir comme l'externalisation vers un prestataire spécialisé de certaines tâches. Les pratiques d'outsourcing sont surtout présentes dans les centres d'appels et de support client.
SAAS	Software As A Service	Application logicielle mise à disposition par un fournisseur de service à distance.
Datacenter	Centre de données	Un centre de données où sont regroupés physiquement un ensemble d'équipements et de ressources informatiques.
Datarecovery Site	Site secondaire du Système d'information (DR)	Site secondaire où sont hébergés des services informatiques qui viennent assurer la redondance d'un site primaire (Datacenter).
DMIA/RTO	Durée Maximale d'Interruption Admissible/ Recovery Time Objective	Représente le temps maximum d'interruption d'un service qu'il est possible de supporter pour une entreprise.
PDMA/RPO	Perte de données Maximale Admissible/ Recovery Point Objective	Valeur qui permet de quantifier le maximum d'information qu'un système d'information peut être amené à perdre suite à un incident.
POC	Proof Of Concept	La preuve d'un concept est une démonstration de faisabilité.
Back Office		Services de l'entreprise qui assure le traitement des opérations internes. Ex : HR, Comptabilité,
VPN	Virtual Private Network	Un réseau privé virtuel est un système qui permet de créer un lien direct entre des ordinateurs distants.
Spin-off	Scission	Scission d'une entreprise : par cette opération une nouvelle entité est créée à partir d'une organisation plus grande.
Cloud	Nuage	Ensemble de ressources informatiques accessibles par internet et dont l'emplacement n'est généralement pas connu par le client.
Hosting	Hébergement	Action d'héberger des ressources informatiques pour le compte de clients et les rendre accessibles via internet.
Monitor(er)	Surveiller	Action de surveiller des processus, des applications ou des ordinateurs/serveurs.
Vlan	Virtual Logical Area Network	Un réseau local virtuel se définit comme un réseau informatique logique et indépendant.

TMG (Microsoft)	Threat Management Gateway	Produit de gamme Microsoft destiné à la sécurité d'un réseau informatique.
DFS-R	Distributed File System - Replication	Système de réplication multimaitre, utilisé entre autre pour la réplication des annuaires Active Directory.
Open space	Espace Ouvert	Espace de travail où les bureaux ne sont pas séparés par des cloisons.
SCI	Système de Contrôle Interne	Se définit comme l'ensemble des activités qui garantissent un déroulement conforme de la marche des affaires.
Switch	Commutateur	Equipement informatique qui permet l'interconnexion d'appareils communicants, ordinateurs, serveurs,etc.
Stack	Empiler	Action de relier plusieurs matériels informatiques dans le but d'en simplifier l'administration. Chaque stack est vu comme un seul élément.
VM	Virtual Machine	Une machine virtuelle est un logiciel informatique qui comme un ordinateur physique exécute un système d'exploitation et des applications.
San	Storage Area Network	Un réseau de stockage spécifiquement dédié à la mutualisation de ressources de stockage.
Firewall	Pare-feu	Matériel ou logiciel permettant d'assurer la sécurité sur un réseau informatique.
HSRP	Hot Standby Router Protocol	Protocole réseau Cisco qui permet d'assurer une continuité de service.
Cisco ESX UCS		Serveur Cisco dédié à jouer un rôle d'hôte pour les produits de virtualisation de gamme VMware.
Appliance	Appareil	Matériel ou logiciel, préconfiguré pour réaliser des tâches spécifiques.
Ticketing	Gestion de tickets	Logiciel qui permet le suivi de l'activité d'un service de support.
Cluster	grappe	Ensemble de serveurs configurés dans le but de réaliser un équilibrage de charge ou une meilleure disponibilité.
Fiber Channel		Support de communication haut débit généralement utilisé entre un ordinateur et un système de stockage.
SCSI		Protocole de communication permettant de relier un ordinateur a un système de stockage.
Fabric	Commutateur/switch	Matériel qui permet de relier des éléments de stockage et des serveurs pour gérer différents aspects (accès, zone, etc.).
SLA	Service Level Agreement	Accord sur un niveau de service, signé entre un client et un prestataire.

INTRODUCTION

Définition : Un Plan de Continuité d'Activité (*PCA*) peut se définir comme étant un processus qui vise à assurer le fonctionnement d'une entreprise en mode dégradé, en cas de sinistre ou de catastrophe majeure.

Les raisons pour entreprendre une démarche de continuité d'activité peuvent être multiples, mais il n'existe pas en Suisse ou en France de cadre légal qui en impose la mise en œuvre, que ce soit pour le secteur public ou le secteur privé. Certaines professions peuvent y être soumises de par leurs autorités respectives, les banques ou les assurances par exemple et d'autres peuvent réaliser la démarche dans le cadre d'une maitrise des risques liées à leurs activités.

On sait aujourd'hui que dans un environnement qui est devenu fortement concurrentiel, la fiabilité et la réputation d'une entreprise sont devenues des notions essentielles. Il est donc important qu'une entreprise puisse prouver qu'elle respecte un certain nombre de règles, de normes et de certifications.

Si l'image de marque et la confiance des clients sont des notions essentielles, c'est qu'on considère que plus de 70 % des entreprises ne survivent pas un arrêt complet de leurs activités pendant plus de 3 jours.

La mise en œuvre d'un plan de continuité d'activité doit donc permettre, par anticipation sur tous les scénarios possibles d'incident et de catastrophe, d'assurer la survie de l'entreprise par le maintien de ses activités clés.

La réalisation de ce projet se décompose donc en plusieurs phases structurées. La phase d'analyse fonctionnelle est la plus complexe car elle nécessite l'intervention et l'adhésion de beaucoup d'intervenants.

Le premier objectif est l'Expression des Besoins en Continuité d'Activité (*EBCA*) afin de pouvoir délimiter un périmètre. Il faut donc énumérer toutes les activités du groupe afin d'identifier celles qui sont essentielles. Il faut aussi formaliser les processus métiers, qu'ils soient internes et externes. Il est fondamental d'inclure dans l'analyse, les échanges et flux d'information avec les prestataires ou les fournisseurs. Un incident chez un partenaire, une cessation d'activité chez un fournisseur peuvent avoir des conséquences importantes. Cette étape est aussi celle que l'on nomme, l'Analyse des impacts métiers (*BIA*), réalisée avec les responsables de chaque service elle permet d'estimer les impacts d'un sinistre majeur.

La phase suivante concerne l'analyse des risques et la notion d'acceptabilité. Dans un premier temps, il faut identifier tous les types de scénarios d'incident ou de catastrophe qui peuvent se produire. Tous doivent être pris en compte : des scénarios qui peuvent sembler rarissimes ou peu probables, comme les catastrophes naturelles, incendie, tremblement de terre, inondation, comme ceux qui sont plus liés à l'actualité : les pandémies par exemple avec le cas H1N1 en Europe, les guerres et attentats : l'exemple des sociétés qui hébergeaient leurs systèmes informatiques principaux et de secours au sein

des sœurs jumelles du World Trade Center est éloquent. Enfin, certains incidents sont plus difficiles à appréhender et c'est souvent le cas lorsqu'on ne maitrise pas ou peu son environnement de fournisseurs ou que l'on a délégué certaines tâches. C'est le cas avec les ruptures d'approvisionnement en matière première, eau, électricité ou la mise en œuvre de sous-traitance, d'outsourcing, d'hébergement mutualisé.

La notion d'acceptabilité permet de déterminer les moyens à mettre en œuvre afin de limiter les effets d'un incident ou d'une catastrophe.

Vient ensuite une phase qui consiste en une analyse des solutions et des moyens de secours. Le système de sauvegarde qui est mis en œuvre, l'externalisation des bandes de sauvegarde, la description du plan de secours informatique, le plan de repli au cas où un site de production serait endommagé. Egalement, la description du plan de secours téléphonique, la mise en œuvre d'un deuxième site ou les ressources sont dupliquées, les mises en œuvres techniques, cluster applicatif, de basculement, etc.

La partie suivante consiste en la gestion de la crise elle-même et à l'organisation de la cellule de crise. Elle nomme les membres de la cellule et définit les rôles de chacun. Elle définit comment se déroule une réunion de crise et comment doit se réaliser le pilotage ainsi que la sortie de crise. Un ensemble de fiches réflexes ont été développées pour permettre des prises de décision rapides et coordonnées. Des annuaires, indispensable pour contacter les responsables et les collaborateurs mais aussi les secours, police, pompier, hôpitaux et tous les prestataires, sont tenus à jour et accessibles au personnel sous format électronique et papier, dans chaque bureaux. C'est dans cette phase aussi que le Plan de communication doit être utilisé. Il définit comment doit se faire la communication du groupe, en interne et en externe afin d'éviter toute dissonance et donner une impression générale de maitrise des évènements.

Enfin, la dernière phase concerne les tests et le maintien en fonction opérationnelle du plan de continuité d'activité, ainsi que la remontée d'information consécutive à un incident ayant eu lieu. Pour être efficace en temps de crise, le PCA doit être testé régulièrement. Pour cela, les moyens techniques doivent être déployés afin de valider leur bon fonctionnement. Les procédures mises en œuvre doivent être mises à jour.

1 CONTEXTE

Le groupe Veltigroup SA est aujourd'hui leader sur le marché suisse des services informatiques à haute valeur ajoutée. Il est composé de 4 sociétés : Veltigroup SA qui pilote le groupe et gère le back office, Lanexpert SA pour les services IT aux grandes entreprises, ITS pour les services IT aux petites et moyennes entreprises et Insentia SA pour le développement d'applications métiers propres. Les infrastructures IT mises à disposition de ces 3 sociétés sont gérées par le Veltigroup IT (*VIT*) qui dépend directement du groupe Veltigroup SA.

Des bureaux sont implantés à Lausanne (*siège social/Datacenter*), Genève (Disaster Recovery Site), Zurich et Berne. Les bureaux de Zurich et Berne regroupent 70 utilisateurs, mais sont uniquement équipés de serveurs de fichiers et d'impressions locaux.

Veltigroup SA emploie un peu plus de 500 spécialistes IT à travers toute la Suisse.

Le groupe, en plus d'offrir des services d'intégration, de conseils, de design et de développement offre des services de support et d'outsourcing. Ces services de support et d'outsourcing ouverts 24h/24 et 7j/7 aux entreprises imposent des contraintes de redondance d'infrastructure et de résilience des données afin de permettre une continuité des services.
L'obligation de respect de la norme ISA3402 pour des clients bancaires est aussi une des causes de la mise en œuvre du plan de continuité de l'activité.

Pour ce qui est du point de départ du projet, il n'existe actuellement aucun plan/processus permettant une reprise ou une continuité d'activité en cas de sinistre. La rédaction de ce document va donc permettre au préalable de définir la stratégie de continuité d'activité du groupe. Il établit et décrit en précisant pour chaque activité essentielle, les niveaux de service retenus ainsi que les durées d'interruption maximale admissible pour ces différents niveaux de service. Il définit les ressources permettant d'atteindre les objectifs de continuité du groupe et tient compte des ressources critiques qui peuvent avoir été perdues pendant le sinistre, jusqu'à la reprise de la situation normale.

Il a été retenu la rédaction d'un PCA unique rassemblant l'ensemble des « risques » pour les sites de Lausanne et Genève uniquement. En effet, les sites de Zurich et Berne, n'hébergent pas d'infrastructure de production.

Il est important de savoir qu'il existe déjà aujourd'hui un site de Datarecovery (*DR*) qui se trouve à Genève et où quelques services ont été dupliqués. Les services de sauvegardes des serveurs sur bandes sont aussi gérés sur ce site.

Les services déjà dupliqués n'entrent pas dans le cadre d'une démarche globale de la mise en œuvre d'un plan de continuité de l'activité et devront être repensés.

Le rôle des différents responsables est défini, les procédures de mise en œuvre du PCA et les moyens nécessaires sont explicités.

1.1 Le groupe Veltigroup SA et les Sociétés qui le composent.

Le groupe est constitué de 4 Sociétés, Veltigroup SA, Lanexpert SA, ITS et Insentia SA et est implanté sur les sites de Lausanne (*site principal, Datacenter*), Genève (*site secondaire, Datarecovery*), Zurich et Berne.

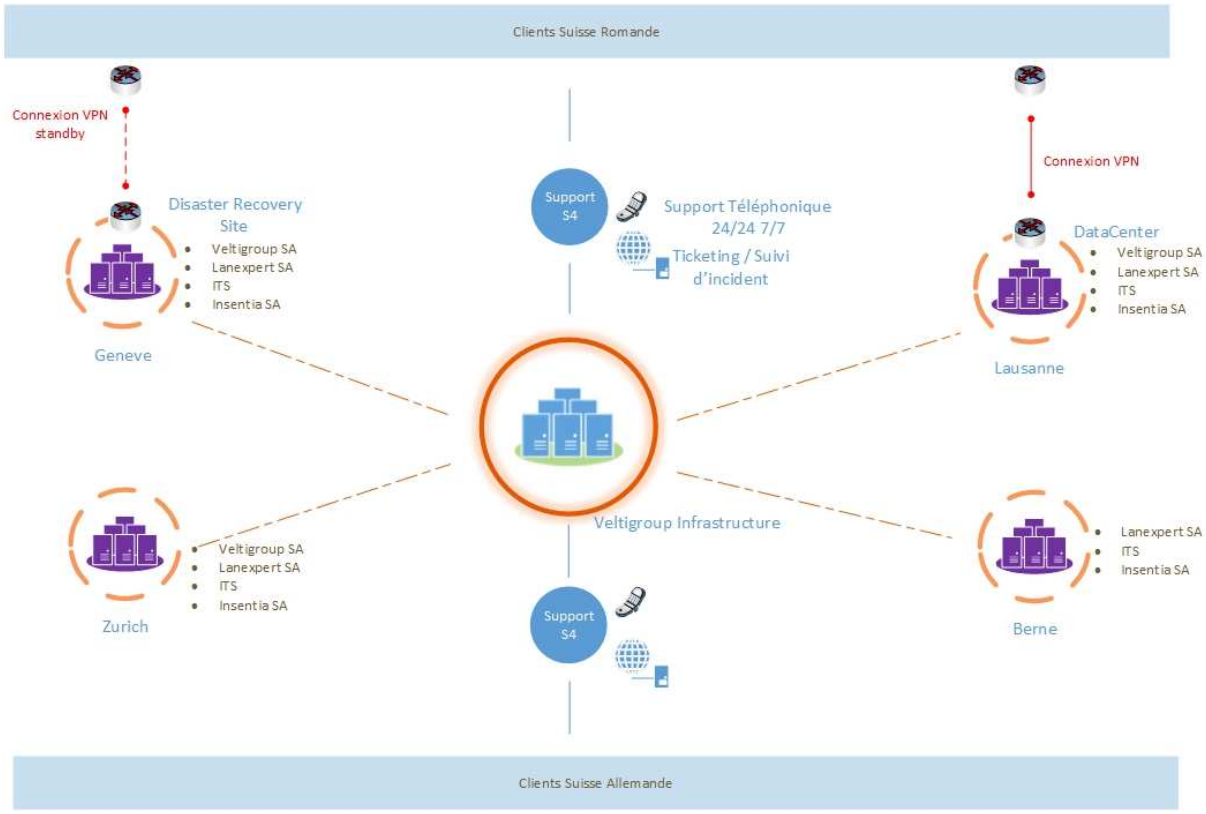


Fig. I : Synoptique du groupe Veltigroup SA

Chaque société du groupe est représentée sur tous les sites. Un service de support 24h/24 7j/7 est accessible aux clients du groupe. L'ensemble des infrastructures informatiques est géré par le VIT (*Veltigroup IT*). Les membres du VIT sont présents sur les sites de Lausanne et Genève et se déplacent régulièrement sur les sites de Zurich et Berne.

Les infrastructures informatiques maintenues par le VIT sont essentiellement composées de serveurs Cisco ESX UCS dans le Datacenter et Datarecovery, 90 % des serveurs Windows et Linux sont virtualisés par les produits VMware.

Une nouvelle société d'hébergement de services et d'infrastructures informatiques (*Cloud et Hosting*) a été créée et fait l'objet d'une scission (*spinoff*). Cette société se nomme Exoscale.

Schéma réseau

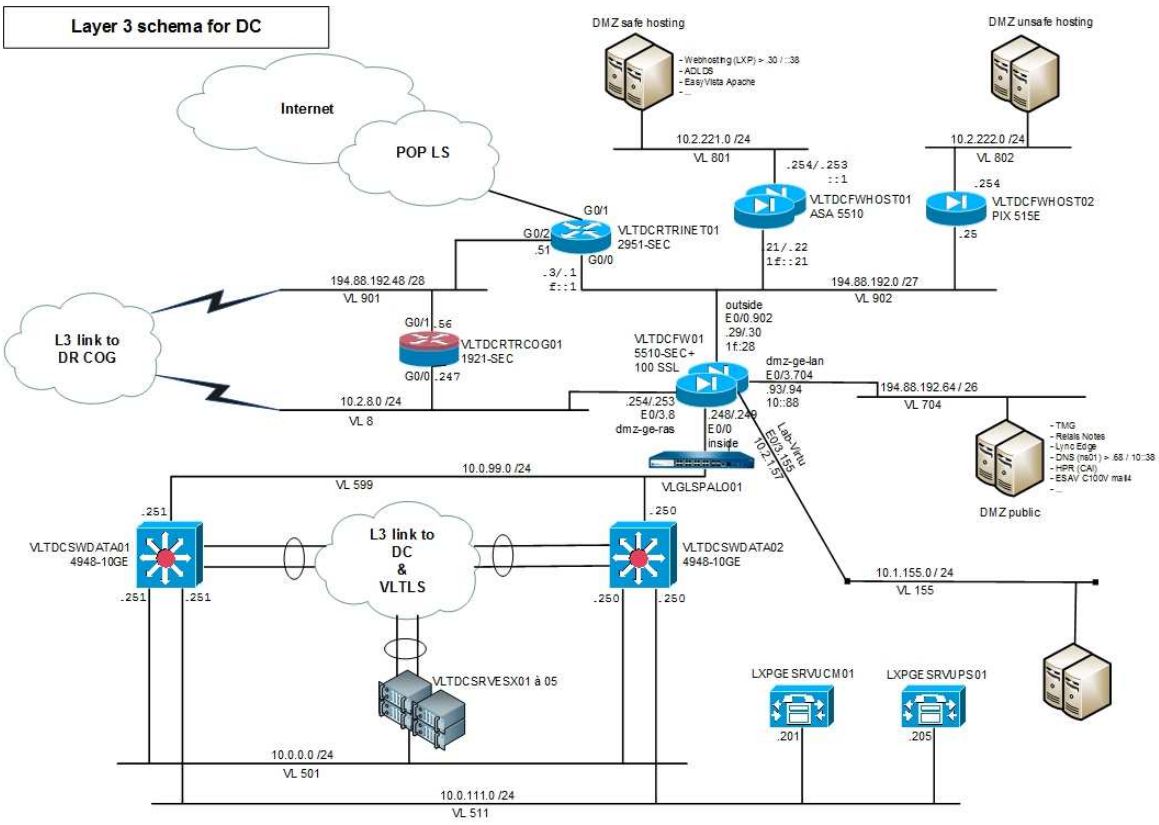


Fig. II : Schéma réseau site Datacenter

Le site Datacenter est composé de cinq hôtes Cisco ESX (*VLTDCSRVESX01 à 05*) connectés sur des switch L3 de données Cisco qui sont stackés. Deux Firewall Cisco ASA en cluster VLTDCFW01 assurent l'analyse des trames et la sécurité. Plusieurs DMZ appelées Publique et Safe Hosting cohabitent. Les VPN avec les clients sont configurés sur deux matériels Cisco configurés avec le protocole HSRP pour assurer leur résilience. Le routeur VLTDCRTRINET01 est le point d'entrée/sortie internet. Le matériel Palo Alto VLGLSPALO01 assure le log des trames internet et répond à une nécessité règlementaire.

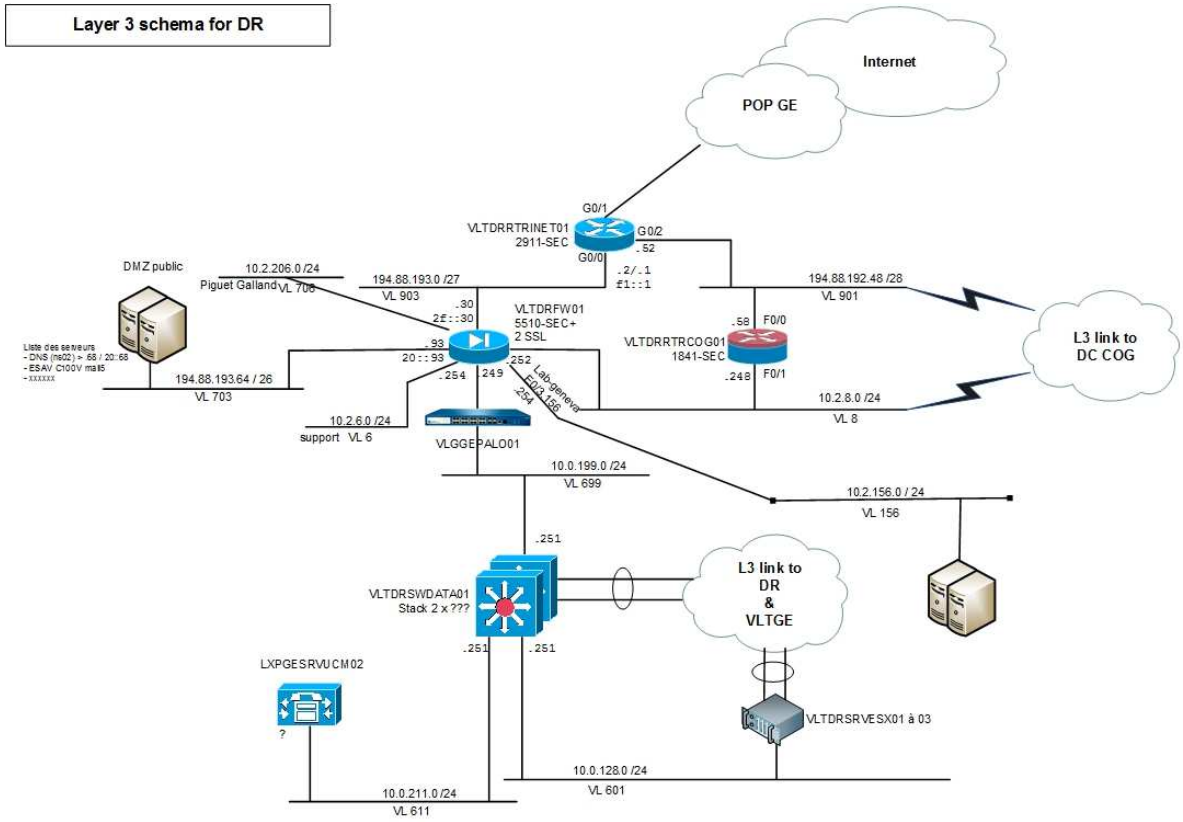


Fig. III : Schéma réseau site Datarecovery

Le site Datarecovery est composé de trois hôtes Cisco ESX (*VLTDRSRVESX01 à 03*) connectés sur des switch L3 de données Cisco qui sont stackés. Deux Firewall Cisco ASA en cluster VLTDRFW01 assurent l'analyse des trames et la sécurité. Plusieurs DMZ appelées Publique et Safe Hosting cohabitent. Les VPN avec les clients sont configurés sur deux matériels Cisco configurés avec le protocole HSRP pour assurer leur résilience. Le routeur VLTDRRTRINET01 est le point d'entrée/sortie internet. Le matériel Palo Alto VLGGEPALO01 assure le log des trames internet et répond à une nécessité règlementaire.

1.1.1 ITS - Information Technologie Services

La société ITS (*Information Technologie Services*) offre essentiellement des services aux petites et moyennes entreprises. Ces services vont de l'aide à la conduite et à la réalisation de projets, à la maintenance de parc informatique (*déploiement, installation, etc.*). De plus, ITS offre un service de surveillance des infrastructures clientes ainsi que de contrôle : contrôle des sauvegardes des données, des alertes, des sécurités, des antivirus, etc.

Un support téléphonique est accessible de 7:00 à 18:30 par une équipe dédiée aux PME.

Des ingénieurs itinérants se déplacent régulièrement chez les clients avec plusieurs objectifs : garder un lien et une communication constante, accompagner correctement, aider à la formation du personnel ou apporter une expertise technique, lors de migration par exemple.

1.1.2 Lanexpert SA (Services aux grandes Entreprises)

Lanexpert SA est composé de 150 ingénieurs, spécialistes en différents domaines informatiques, conduite de projets, réseaux, stockage, virtualisation, etc. et est orienté exclusivement vers les services aux grandes entreprises. L'entreprise dispose d'un support téléphonique accessible, 7 jours sur 7 et 24h sur 24h aux clients francophones, anglophones et germanophones. Un centre de formation permet la formation du personnel informatique, interne et externe dans les locaux de l'entreprise à Lausanne, Genève et Zurich. De la même manière que la société ITS, Lanexpert offre des services de surveillance des infrastructures, de contrôle, d'aide et d'accompagnement du personnel.

1.1.3 Insentia SA

Insentia SA, est la société du groupe orientée développement d'applications, elle est le résultat de plusieurs fusions (*Perhalion SA, pragmantic, Epyx SA, CAI*). La société se compose d'une centaine d'ingénieurs spécialisés en développement. La société développe entre autres des services applications « logiciels en tant que service », Software As A Service (*SAAS*), des applications mobiles, des applications web, etc.

2 LE PLAN DE CONTINUITÉ D'ACTIVITÉ

La mise en place et le maintien du PCA se réalisent en six étapes successives. Ces six étapes sont plus ou moins difficiles à mettre en œuvre, car elles nécessitent à chaque fois la participation de plusieurs intervenants ainsi que la validation de la direction du groupe.

2.1 Le Cycle de vie du PCA

1. **L'identification des fonctions/activités essentielles à la poursuite des activités de l'entreprise.**
2. **L'identification des technologies maîtrisées et des choix retenus par l'entreprise.**
3. **La définition des solutions de secours ou du Plan de Secours Informatique(PSI).**
4. **La définition de la gestion de crise.**
5. **Réalisation des tests.**
6. **Maintien en condition opérationnelle.**

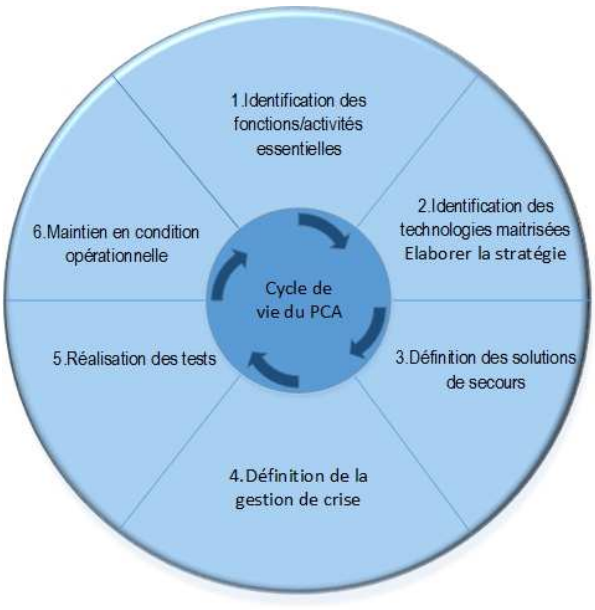


Fig. IV : Cycle de vie du PCA

2.2 Définition du périmètre

Cette étape a consisté à définir le périmètre des actifs critiques (*activités et processus, organisations et infrastructures*) de l'entreprise à maintenir démarré en priorité en cas d'incident ou de sinistre. Cela a été validé par la direction du groupe lors d'un comité de pilotage (*COPIL*).

Pour chacune de ces activités (*applications informatiques et/ou processus*), une Durée Maximale d'Interruption Admissible (*DMIA*), également connu sous le nom de Recovery Time Objective (*RTO*) et une Perte de Données Maximale Admissible (*PDMA*) connu sous le nom de Recovery Point Objective (*RP*) ont été définis. La DMIA/RTO peut se traduire par la durée maximale d'interruption d'un service offert aux usagers que l'on juge admissible avant que l'entreprise n'en supporte des effets trop lourds, en terme financier ou d'image de marque. La PDMA/RPO représente la durée maximum d'enregistrement des données qu'il est acceptable de perdre, c'est-à-dire le temps qui s'est écoulé depuis que la dernière sauvegarde a été réalisée.

Il convient donc de se poser les questions suivantes, pour calculer une DMIA et une PDMA :

DMIA : Pendant combien de temps pouvons-nous supporter de nous passer de telle application et/ou tel processus. Par exemple, pendant combien de temps pouvons-nous supporter qu'un client n'ait pas accès à la partie support/web du groupe et donc accès à la gestion de ses tickets.

PDMA : De combien de temps doit dater la dernière sauvegarde qui a été réalisée, pouvons-nous supporter de perdre par exemple, les 4 dernières heures de travail, les 8 dernières heures de travail, etc. donc plus le RPO est faible, plus la fréquence de sauvegarde des données devra être rapide.

Fig. V : Positionnement du DMIA/PDMA dans un cas de sinistre (source : http://moodle.insa-toulouse.fr)

Pour mener la réflexion plus en avant, plusieurs paramètres ont été également pris en compte et un croisement de ces paramètres a été effectué. La criticité d'une application, une liste des différents types de risques auxquels ces applications sont soumises, un niveau d'impact de ces risques, une évaluation de la probabilité et de la récurrence de ces évènements et donc un niveau d'importance qu'un risque fait courir sur notre qualité de service.

2.2.1 Énumération des activités par service

La 1ère étape concerne l'identification des fonctions et de toutes les activités réalisées par le personnel. Elle pose les fondations de la démarche qui donnera lieu plus tard à l'élaboration des différents plans de secours et à la mise en place des solutions de continuité de l'activité pour l'entreprise. C'est celle qui a été la plus compliquée et la plus longue à mettre en œuvre.

Cette étape requiert la participation de tous les responsables de services. Une fois cette liste réalisée et synthétisée il a fallu ordonner ces activités par importance. Essayer de dégager quelle activité est stratégique ou quelle activité l'est moins. J'ai pu constater qu'il est compliqué, voire très compliqué, de demander à un responsable de service de quelle activité il pourrait se passer ou à minima pour combien de temps au maximum il pourrait s'en passer. Tout étant à leurs yeux très important. La hiérarchisation des activités prioritaires est aussi compliquée. Toutefois, en expliquant la nature du projet et la réalisation d'évènements exceptionnels qui en résulte, nous sommes parvenus à des résultats.

Ces résultats, pour permettre de valider plus tard les décisions techniques, ont été exposés lors d'un Comité de Pilotage (*COPIL*), qui est une réunion mensuelle qui rassemble l'ensemble des directions des sociétés du groupe.

Les deux types d'impacts que nous avons choisi de prendre en compte sont l'impact financier direct d'une rupture de service et celui de la réputation ou de l'image du groupe (*Tableau I)*, sur une même échelle de temps qui représente la durée de l'interruption maximale (*Tableau II)*.

L'impact financier a donc été calculé à partir de plusieurs paramètres, le temps d'indisponibilité supposé (*c'est-à-dire le temps d'indisponibilité maximum avant le redémarrage d'un service par n'importe quel moyen, utilisation des bandes de sauvegarde, nouveau matériel, temps d'intervention d'un prestataire dans le contrat, etc.),* le chiffre d'affaires annuel du groupe, rapporté aux sociétés et pondéré par service si nécessaire. Le chiffre obtenu permet ainsi de classer l'incident dans un tableau à quatre entrées (*impact financier, faible, moyen, élevé et critique*) (*Tableau III*).

Tableau I : Tableau de pondération

	Impact financier lié à une rupture de service	Effet négatif sur l'image du groupe
Service Ressources Humaines	1	1,2
Service Marketing	1	1,5
Service Vente	1,5	1,5
Service Comptable	1,2	1
Service Administratif	1,5	1
Service Support S4	1	1,5
Service VIT	1	1
Consultants	1,5	1,5

Le présent tableau a pour but de fixer une pondération quant aux conséquences d'un incident survenu dans l'un des services cités.

Tableau II : Tableau d'évaluation de durée d'un incident

Incident/sinistre	description	Temps d'indisponibilité maximal
Défaillance de la climatisation :	Son arrêt peut provoquer le dysfonctionnement ou l'arrêt du SI	4h
Perte d'alimentation énergétique :	Fermeture du fournisseur d'électricité	8h
Perte des télécommunications :	Absence de réseau téléphonique	4h

Tableau III : Tableau d'impact financier

Niveau	Impact
Faible	Impact financier est faible < 10 KCHF Touche un nombre de clients/prestataires peu élevé
Moyen	Impact financier est moyen 10 KCHF<> 100KCHF Touche quelques clients ou prestataires Les médias spécialisés sont informés
Elevé	Impact financier est élevé > 100KCHF Touche beaucoup de clients ou prestataires Les médias grand public sont informés
Critique	Impact financier critique > 1MCHF arrêt de l'activité Tous les clients sont impactés Crédibilité du groupe en péril

Pour expliquer la pondération, le service vente par exemple bénéficie d'une pondération plus élevée que celui des ressources humaines. Non pas que nous avons évalué un degré d'importance, mais nous avons jugé que l'impossibilité de finaliser une vente avait plus d'impact financier direct que l'impossibilité de réaliser une embauche par exemple. À l'inverse, la réputation ou l'image du groupe peut se trouver fortement détériorée auprès d'un futur collaborateur si son embauche, qui était prévue, ne peut se réaliser le jour dit suite à un incident quelconque.

A noter que nous n'avons pas pris en compte tous les aspects contractuels nous liant à nos clients et les aspects de niveau de service (*SLA, Service Level Agreement*) non respectés. Nous n'avons non plus pas tenu compte de paramètres liés au contrat de travail mettant en cause la responsabilité pénale d'un employé ou de l'employeur.

J'ai donc élaboré un premier tableau, par service dans lesquels sont listées exhaustivement toutes les activités réalisées par le personnel.

Tableau IV : Activités du service Ressources Humaines - Responsable du Service : M.L Joncour

Activités du service Ressources Humaines
Gestion de la base de données des candidats à jour.
Recherche, qualification, présélection des candidats à présenter aux gestionnaires d'embauche.
Gestion du processus d'entrevue/d'embauche complète.
Assurer la liaison entre les gestionnaires d'embauche et les experts (les descriptions des postes de travail, la gestion de la publicité des positions ouvertes et la stratégie de recrutement définie).
Organisation d'événements de recrutement.
Mise en réseau au sein du marché pour atteindre et attirer de nouveaux candidats, la vente de l'entreprise, l'emploi et la possibilité de carrière à travers la connaissance de la société, sa culture, ses avantages et les produits.
Gestion des activités de recrutement de l'Université.
S'assurer que toutes les initiatives de recrutement sont conformes aux exigences légales.
Assurer la liaison avec le directeur d'embauche et de représentants RH des bureaux distants pour préparer des offres d'emploi et de s'assurer que tous les documents de préemploi sont fournis par les candidats avant le début de l'embauche.
Participer à l'administration de toutes les assurances sociales et accidents « déclarations » (c. allocations familiales, LPP, etc…, entrées / sorties) – changements.
Aider dans le processus des nouveaux entrants (logistique, planification, etc.).
Participer à des demandes ou des renouvellements de permis de travail.
Planification, réunions/dépôt appropriées de divers documents RH, des fiches de suivi de la surveillance et de la correspondance liées au département.
Gestion des offres d'emploi sur différents médias (Intranet, Internet, joboards).
Gestion du planning des meetings/entrevues avec les candidats (MS Outlook).
Assistance administrative pour préparer ou mettre à jour des présentations PowerPoint, des tableaux Excel ou des documents Word.

Tableau V : Activités du service Marketing - Responsable du Service : Alexandre Cudre-Mauroux

Activités du service Marketing
Gérer la présence du groupe dans les réseaux sociaux tels que Facebook, Twitter et autres sites communautaires similaires, l'affichage sur les blogs pertinents.
Communiquer dans des espaces de médias sociaux, l'engagement dans le dialogue et répondre aux questions, le cas échéant.
Identifier les menaces et les opportunités dans le contenu généré par l'utilisateur autour de nos services ou entreprises, rapport aux parties concernées.
Créer du contenu pour les flux dans divers sites de médias sociaux.
Générer du contenu pour de multiples services/entreprises sur une base quotidienne.
Participer dans les conversations qui entourent notre contenu et nos services, répondre à des commentaires, être un médiateur.
Mener des recherches par mot clé, y compris de catalogage et d'indexation cibles, phrases clés.
Faire des recommandations et des plans pour la création et l'amélioration des campagnes de médias sociaux.
Mesurer l'impact des initiatives de médias sociaux, analyser, examiner et faire rapport sur l'efficacité des campagnes dans un effort pour maximiser les résultats.
Surveiller les tendances en outils de médias sociaux, tendances et applications.
Faire des recommandations et des plans pour la création et l'amélioration des campagnes de médias sociaux.
Définir, développer et mettre en œuvre une stratégie de communication des produits.
Identifier les besoins d'industrialisation et de promotion des produits et services des sociétés du Groupe.
Établir le Marketing mix en collaboration avec les personnes en charge du Développement du Business.
Créer et gérer la production de supports marketing, tels que brochures, plaquettes, flyers en collaboration avec des agences externes si nécessaire.
Définir, développer et mettre en œuvre une stratégie de communication des produits.
Gérer des campagnes publicitaires dans différents médias (presse, sociaux, web, etc.).
Analyser le succès commercial de nos produits avec les outils et KPI's adéquats.
Rester à l'écoute du marché au travers d'une veille technologique de nos différents concurrents.

Tableau VI : Activités du service Vente - Responsable du Service : Alexandre Cudre-Mauroux

Activités du service vente
Développement du portefeuille de service S4 et de la base clients en Suisse romande.
Identifier le potentiel de développement du marché en collaboration avec l'équipe de Vente.
Définir des mesures de Marketing sur les services S4 en collaboration avec l'équipe Marketing.
Participer activement dans la définition des stratégies de vente et des feuilles de route pour la mettre en œuvre.
Élaborer les offres en collaboration avec les collègues du groupe.
Négocier les contrats de prestations avec les clients.
S'assurer de la bonne exécution des projets de transition.
Assurer la gestion commerciale d'un ensemble de clients.
Identifier et sélectionner les comptes de Veltigroup potentiels dans la région suisse alémanique.
Être responsable de la planification d'entreprise, le développement de compte et des rapports financiers des comptes nominatifs.
Être responsable des objectifs financiers.
Établir des relations étroites avec les clients finaux.
Recueillir et analyser les besoins des comptes basés sur des visites régulières des clients nouveaux du marché et 360° TIC, construire et examiner des stratégies de comptes.
Suivre le marché et analyser les besoins et les demandes des clients en termes de services et de solutions dans les domaines ECM et CS.
Évaluer les offres technologiques concurrentes afin de positionner notre société sur des demandes clientes précises et sur les évolutions du marché en général.
Gérer un portefeuille de clients existants et prospecter le marché afin de développer de nouveaux clients.
En collaboration avec les équipes techniques, négocier et valider les aspects contractuels.
rédiger des offres en adéquation avec les besoins et exigences du client.
Promouvoir l'offre de services de consulting et d'engineering Insentia, ainsi que l'offre de trading en prospectant les clients et le marché dans ces domaines.
Grâce à une base clients existante, identifier de nouvelles opportunités de projets et les matérialiser en tant que succès commerciaux.
Menez également à bien des activités de prospection sur le marché romand.
En collaboration avec les équipes d'ingénieurs, contribuer à concevoir les meilleures solutions.
Prendre part à la définition de la stratégie commerciale de la société.

Tableau VII : Activités du service Comptabilité - Responsable du Service : Joseph Ayuso

Activités du service comptabilité
Gérer la comptabilité du groupe et des sociétés.
Facturation des services, des affaires de négoce, des fournisseurs et des paiements.
Assurer le suivi des postes ouverts débiteurs et créanciers.
Contrôler et traiter les frais généraux, notes de frais, etc.
Établir les décomptes TVA.
Clôtures mensuelles et établissement des tableaux de bord.
Analyse et documentation des tableaux de bord.
Participation à la préparation des bouclements annuels.

Tableau VIII : *Activités du service Administratif* - Responsable du Service : Marc-Antoine Busigny

Activités du service Administratif
Assister l'équipe de vente dans l'établissement des devis.
Contrôler et enregistrer les commandes de ventes.
Sélectionner les fournisseurs et gérer les achats.
Assurer le suivi des commandes et livraisons en relation avec la planification des projets.
Établir les décomptes TVA.
Établir et gérer les contrats de maintenance et leur renouvellement.
Assurer la bonne tenue informatique des dossiers.
Gérer la relation administrative avec les partenaires et fournisseurs.
Documenter et tenir à jour les procédures de travail relatives aux partenariats.
Gérer les catalogues d'articles pour vos produits.
Contribuer aux activités administratives générales des sociétés du groupe.
Gérer avec autonomie et responsabilité les dossiers et interagir avec les autres services du Groupe, par exemple avec le service comptabilité.

Tableau IX : Activités du service Support S4 - Responsable du Service : Philippe Vessillier, Xavier Bandeville

Activités du support S4
Assurer l'assistance et le support téléphonique aux utilisateurs.
Assurer la résolution d'incidents de 1er et 2ème niveaux.
Assurer un temps de réponse adaptée et un service de haute qualité.
Assurer l'escalade technique vers les centres de compétences.
Assurer la satisfaction du client en apportant des solutions efficaces à l'équipe informatique interne de nos clients.
Assurer le suivi des incidents jusqu'à leur clôture.
Gérer l'administratif et le suivi des activités à l'aide outil ITSM (EasyVista).
Gérer de façon professionnelle et optimale la relation avec nos Clients.
Maintenir et développer des compétences professionnelles et une expertise technique.
Accompagner l'évolution des besoins de nos clients par des propositions d'améliorations des infrastructures en collaboration avec nos architectes.
Être responsable des infrastructures IT en place chez nos clients, gérer de manière efficiente les opérations, la résolution des incidents et les demandes de changements.
Maintenir l'ensemble des compétences du personnel sur les technologies prises en charge.
Contribuer au respect de nos engagements, des niveaux de services attendus et fournir une qualité de service exemplaire.

Tableau X : Activités du service VIT - Responsable du Service : Claudio Simone

Activités du service VIT
Assurer l'assistance et le support téléphonique aux utilisateurs.
Assurer la résolution d'incidents de 1er et 2ème niveaux.
Assurer un temps de réponse adaptée et un service de haute qualité.
Assurer l'escalade technique vers les centres de compétences.
Assurer la satisfaction du client en apportant des solutions efficaces à l'équipe informatique interne de nos clients.
Assurer le suivi des incidents jusqu'à leur clôture.
Gérer l'administratif et le suivi des activités à l'aide outil ITSM (EasyVista).
Gérer de façon professionnelle et optimale la relation avec nos Clients.
Maintenir et développer des compétences professionnelles et une expertise technique.
Être responsable des infrastructures IT.
Maintenir l'ensemble des compétences du personnel sur les technologies prises en charge.
Contribuer au respect de nos engagements, des niveaux de services attendus et fournir une qualité de service exemplaire.

Tableau XI : Activités des Consultants - Responsable du Service : Yama Zakarya

Activités des consultants
Gérer de manière efficiente les opérations, la résolution d'incidents et les demandes de changements de nos clients.
Accompagner l'évolution des besoins de nos clients par des propositions d'améliorations des infrastructures en collaboration avec nos architectes.
Être sensible à l'industrialisation des processus et identifier les activités qui peuvent être automatisées ou optimisées.
Gérer de façon professionnelle et optimale la relation avec nos clients.
Contribuer au respect de nos engagements, des niveaux de services attendus et fournissez une qualité de service exemplaire.
Maintenir et développer vos compétences professionnelles et une expertise technique.
Responsable de notre prestation de solution ITSM — Mettre en œuvre l'architecture technique nécessaire. — La mise en œuvre et la formalisation des processus ITIL. — Intégration de solution ITSM au sein de l'environnement informatique de nos clients. — Paramétrage, les scripts, les essais et la mise en forme. — La documentation de mise en œuvre d'écriture.
intervention sur site pour des projets ITSM, le fonctionnement, la migration, le déploiement, etc.
Prise en charge de l'équipe des ventes dans les activités de prévente (preuve de concept...).
Être capable de travailler indépendamment de la définition du champ d'application sur certains projets.
Être le responsable technique de l'infrastructure informatique (réseau, serveurs, postes de travail, sécurité, backup…) en tant que personne de contact principale de vos clients.
Assurer l'administration et la maintenance proactive à distance et sur site des systèmes.
Être le responsable technique et réaliser des projets pour les clients assignés.
Assurer l'évolution des solutions d'infrastructure du système d'information (tenue à jour de l'inventaire matériel et logiciel et de la documentation opérationnelle, rôle de conseiller pour le client).
Gérer l'architecture logicielle, le développement, la personnalisation, l'intégration ainsi que la gestion de projet technique pour répondre aux attentes des clients et les objectifs du projet qui sont dans la portée et le budget.
Fournir un leadership sur les meilleures pratiques pour la conception architecturale, avoir une compréhension approfondie de l'intégration d'applications d'entreprise.
Diriger les avis d'architecture et de design pour des projets axés sur la validation technique, les contraintes de déploiement, et le ciblage de nouvelles ou importantes modifications.
Jouer un rôle de premier plan dans le développement des compétences et des connaissances techniques des membres de l'équipe et les clients.
Effectuer des activités de soutien et de maintenance liés aux processus de passation des marchés.
Avoir une vue d'ensemble des processus.
Collaborer avec les analystes d'autres flux d'affaires pour définir l'interaction au sein des processus de bout en bout.
Participer et fournir une assistance dans les tests de processus de bout en bout.
Former les utilisateurs clés et de préparer le plan de formation pour les utilisateurs finaux.
Assurer les activités de support et de maintenance selon les SLA définis.
Identifier les projets, les demandes de changement et de les hiérarchiser.
Évaluer les besoins de l'entreprise en collaboration avec les secteurs d'activité.
Recueillir, spécifier et exigences d'affaires.

Ensuite, une fois ce premier tableau obtenu (*avec le concourt de chaque responsable de service*), j'ai pu lister les applications informatiques qui étaient utilisées pour réaliser ces activités. Quand ceci a été fait, j'ai de nouveau sollicité chaque responsable de service afin d'évaluer avec eux quelles activités pouvaient être jugées comme critiques ou non (*Tableau XII à XVI*).

De plus, des valeurs de Durée Maximale d'Interruption Admissible (*DMIA*), et de Perte de Données Maximale Admissible (*PDMA*) ont été définies quand il y avait matière à les définir. On ne peut pas toujours définir de PDMA, par exemple sur le service de passerelle mail (*Cisco SMTP Ironport*), il n'y a pas de sauvegarde d'un état qui permette un retour à un état précédent.

Tableau XII : Application Lotus Notes

Application/service	Activités/Fonction	Description	Criticité	DMIA	PDMA
Lotus Notes	Projets/Rubriques	Gestions des Projets, rubriques	O	8	8
Lotus Notes	Work Reports	Rapports de travail des employés	O	8	8
Lotus Notes	Expenses / Travel / Personal Allowance	Gestion des frais/déplacements/remboursements/allocations personnelles	N		8
Lotus Notes	Invoices	Facturation	O	8	4
Lotus Notes	Off-Work	Requête jour non travaillé	N	8	8
Lotus Notes	HR - Payroll info	Gestion l'employé/salaire/Bonus	N	8	8
Lotus Notes	HR	HR info, entretien annuel, congés, infos financières	N	8	8
Lotus Notes	HR	cycle de formation/CV	N		8
Lotus Notes	Workflows/Approvals	Utilisation de workflows et cycle d'approbation	N	8	8
Lotus Notes	Password	Gestion des mots des passes du groupe	O	4	4

Tableau XIII : ERP Microsoft Dynamics Navision

Application/service	Activités/Fonction	Description	Criticité	DMIA	PDMA
Dynamics NAV 4.0	Contacts	Gestion des Contacts	O	4	8
Dynamics NAV 4.0	Sales	Offres/Gestion des offres de vente	O	8	8
Dynamics NAV 4.0	Maintenance	Matériel & Logiciels — maintenance pour client	O	8	8
Dynamics NAV 4.0	Purchase	Gestion des ordres d'achats	O	8	4
Dynamics NAV 4.0	AR	Comptes recevables (clients, factures)	O	8	0
Dynamics NAV 4.0	AP	Comptes Payables (fournisseurs, factures)	O	8	8
Dynamics NAV 4.0	GL	Grand livre des comptes	O	8	0
Dynamics NAV 4.0	Budget	Budgétisation	O	8	4
Dynamics NAV 4.0	Assets	Gestion des évaluations	O	8	8
Dynamics NAV 4.0	Payroll	Gestion de la paie des salaires suisses	N	4	

Tableaux XIV : Communication

Application/service	Activités/Fonction	Description	Criticité	DMIA	PDMA
Communication	Lync	Outil interne de communication	N	8	
Communication	Remote Call Control	Option d'appel rapide	N		
Communication	Share desktop	Partage d'écran Lync	N	8	
Communication	Video conferencing	Outil de conférence Tandberg vidéo	N	8	
Communication	Directory access	Disponibilité des listes d'adresses de tous les clients et contact du groupe	N	8	

Application/service	Activités/Fonction	Description	Criticité	DMIA	PDMA
Messagerie	Outlook	Client de messagerie	O	4	4
Messagerie	Spam management	Passerelles SMTP — Ironport	O	4	
Messagerie	Webmail	Accès à la messagerie via navigateur	N	8	
Messagerie	Activesync	Synchronisation des téléphones portables	N	8	
Messagerie	Mail to SMTP	Passerelle SMS	N	8	
Messagerie	Mail archiving	Archivage Enterprise vault de la messagerie	N	8	
Messagerie	Directory access	Disponibilité des listes d'adresses de tous les clients et contact du groupe	N	8	

Application/service	Activités/Fonction	Description	Criticité	DMIA	PDMA
Telephony	Mobility extension	Profils téléphonique permettant la mobilité	N	8	
Telephony	Call Center	Logiciel utilisé par le support pour gérer la téléphonie	O	1	
Telephony	Directory services	Annuaire Global	N	8	

Application/service	Activités/Fonction	Description	Criticité	DMIA	PDMA
Conference room	Connectivity	Disponibilité du câblage	N	1	
Conference room	Conferencing	Outils pour conférence (Lync, You send it, Meet me)	N	4	
Conference room	Projection	Qualité et résolution	N	8	
Conference room	Equipment	équipements (Tableau blanc, TV, projecteurs)	N	8	

Tableau XV : Connexion

Application/service	Activités/Fonction	Description	Criticité	DMIA	PDMA
Remote access	SSL VPN	Client Cisco Anyconnect	N	4	
Remote access	Web VPN	VPN utilisé dans un navigateur (login.veltigroup.com)	N	8	
Remote access	Outlook	Sécurité	N	4	
Remote access	Lync	Sécurité et accès	N	8	
Remote access	Microsoft TMG	Sécurité et accès	O	4	

Application/service	Activités/Fonction	Description	Criticité	DMIA	PDMA
Wi-Fi	wifiguestlan	Wifi pour les inviter/clients/,etc.	N	8	
Wi-Fi	wifidatavit	Wifi pour la production/collaborateurs	O	2	
Wi-Fi	wifitraining	Wifi pour la formation	N	8	

Tableau XVI : Application diverses

Application/service	Activités/Fonction	Description	Criticité	DMIA	**PDMA**
Reporting Services	NAV Reporting	Compte-rendu basé sur les données NAV (Bid, SO, PO, Maintenance, budget,)	N	8	
Reporting Services	Notes Reporting	Rapports basés sur les entrepôts de données	N		
Reporting Services	Easyvista Reporting	Rapport EasyVista	N		

Application/service	Activités/Fonction	Description	Criticité	DMIA	PDMA
Intranet	Intranet	Site Intranet du groupe	O	4	4
Intranet	DynaPM	Gestion de projets	O	8	
Intranet	CLIEF	Gestions des clients	O	8	8
Intranet	Sales Dashboard	Tableau de gestion des ventes Outils pour KAM[1], AM[2] et bizdevs[3]	N	8	

Application/service	Activités/Fonction	Description	Criticité	DMIA	PDMA
Internet	Bandwith	performance Internet (Cacti)	O	2	
Internet	Security	restriction Internet — non implémenté	N		

Application/service	Activités/Fonction	Description	Criticité	DMIA	PDMA
File	Security	Sécurité des serveurs de fichiers	N		
File	Organization	Connexion des lecteurs réseaux	N	4	

Application/service	Activités/Fonction	Description	Criticité	DMIA	PDMA
Application delivery	Citrix	Publication d'applications a distance	O	4	
Application delivery	Web interface	Accés Citrix	O	4	

Application/service	Activités/Fonction	Description	Criticité	DMIA	PDMA
Support assistance	Remote desktop	Applications available for remote assistance	N	4	
Support assistance	Share big file	Partage de fichiers volumineux (you send it)	N	8	

Application/service	Activités/Fonction	Description	Criticité	DMIA	PDMA
Intranet VIT	Documentation	Nombre et qualité de la documentation VIT	N	8	8
Intranet VIT	Information	Communication et accessibilité	N		

Application/service	Activités/Fonction	Description	Criticité	DMIA	PDMA
Workstation	Deploiement	Plateforme de déploiement d'ordinateur (boot PXE)	N	8	
Workstation	Software	Utilitaires disponibles dans le DFS : DFS\DSL\IT	N	8	

Application/service	Activités/Fonction	Description	Criticité	DMIA	PDMA
EasyVista	ITSM (Information Technology Service Management)	ITSM pour le centre de support Opérationnel Veltigroup	O	4	4
Kasaya	ITSM	ITSM pour le centre de support ITS	O	4	4
Reporting Services	Sales Dashboard	Tableau de reporting	N	8	8
Excel	Management KPI	Information et résultat financier	N	8	
Print	Availibility	Accessibilité des imprimantes et liaison sous Citrix	N	4	
Network	Connectivity	Disponibilité du câblage	O	1	
Office physical access	Badge	Badge d'accès aux bureau	O	1	
Extention Data Center	LAB access	Accès à la partie Cloud du groupe pour LAB	N	4	

Pour donner un exemple concret du calcul de l'impact d'un incident, comme un arrêt des climatisations dans la salle du Datacenter qui impacterai le service RH de la société Lanexpert.

Chiffre d'affaire du groupe (*ou de la société du groupe si il y a lieu*) x pondération Financier & pondération image /Temps d'indisponibilité maximum

Evaluation du coût financier

$$\left(80\ M \times \frac{1}{240\ jours\ ouvrés}\right)\Big/_{24\ Heures} = 13\,000\ CHF$$

Evaluation du coût en termes d'image

$$\left(80\ M \times \frac{1{,}2}{240\ jours\ ouvrés}\right)\Big/_{24\ Heures} = 16\,666\ CHF$$

Les chiffres obtenus permettent d'évaluer le coût théorique d'un incident. Ici on peut constater un coût en termes d'image plus important qu'un coût purement financier. On peut donc classer cet incident dans les impacts « moyen » dans le tableau d'impact financier (*Tableau III*).

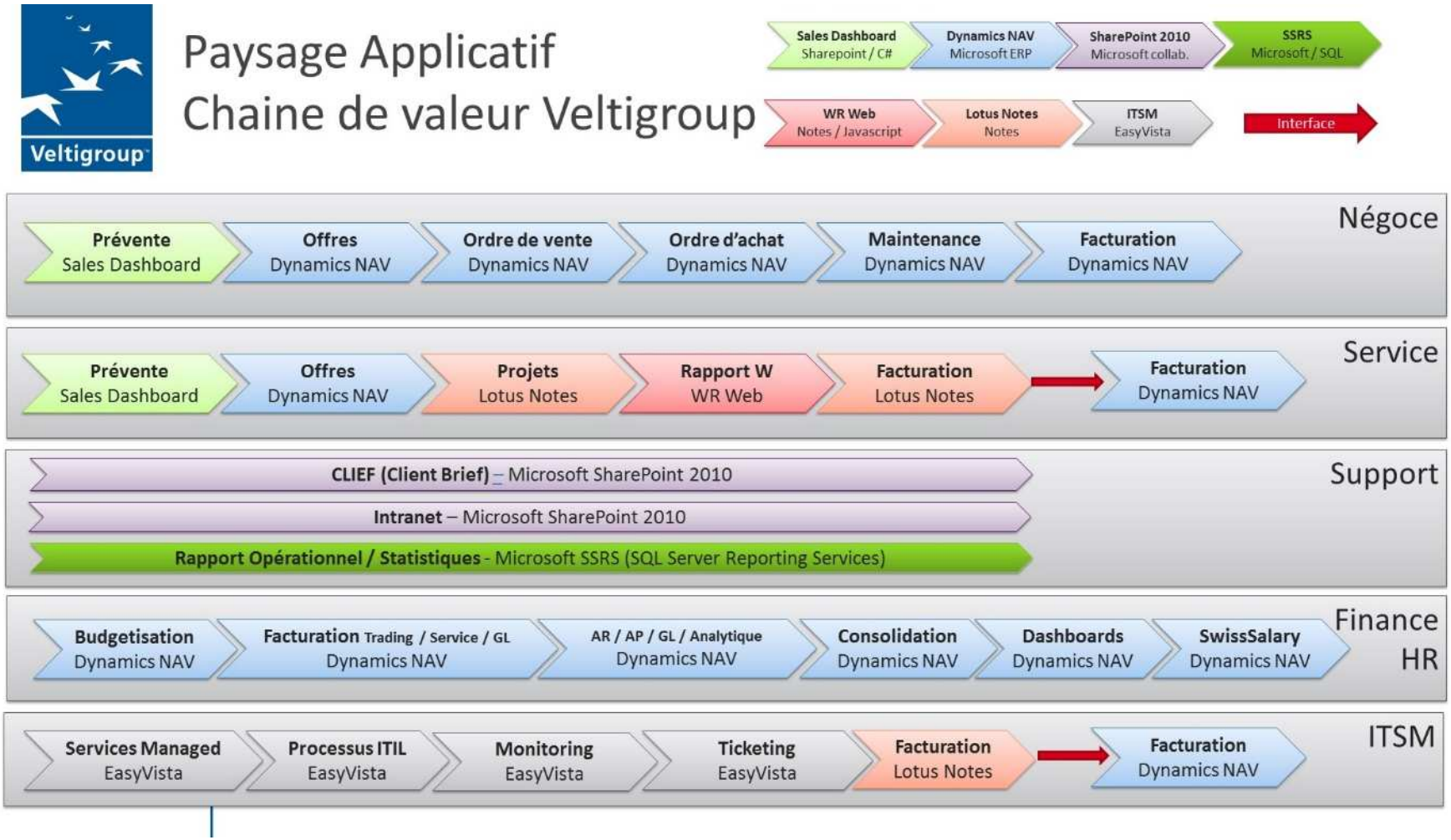


Fig. VI : Cartographie des processus critiques

2.2.1.1Création des tableaux : niveaux d'importance, niveaux de probabilité, niveau d'impact et de synthèse

Cette étape de la conception du Plan de continuité d'activité fait déjà partie de l'analyse des risques. En m'appuyant sur le travail de M. Jean-Claude JACQUIOT sur l'analyse des risques [*Source : http://www.case-france.com/*] et de la définition même du risque, j'ai essayé de bâtir des grilles et tableaux de gravité/probabilité.

Définition du risque : Le risque peut se définir comme l'association d'un danger, de sa probabilité, de sa gravité et de son acceptabilité. L'objectif ici est donc de trouver par quel moyen il était possible de déterminer quel type d'incident/catastrophe, en termes de gravité et de probabilité, nécessiterait qu'on y investisse du temps et de l'argent.

Le 1er tableau décrit quels sont les différents niveaux d'importance d'un risque, du niveau le plus faible (1) c'est-à-dire un risque qui a déjà été évalué, qui est connu et donc à prendre en compte, mais qui ne met pas le groupe en danger. Au niveau le plus fort (5), qui est un risque catastrophique, le risque a été détecté, il est géré et des contrôles ont lieu régulièrement pour s'assurer que des contre-mesures sont en place.

Tableau XVII : Niveau Importance : combinaison de la probabilité et de l'impact.

1	Négligeable	Habituellement, un risque identifié et évalué comme n'étant pas important.
2	Bas	Pas une priorité, mais garder à l'esprit au cas où il y a un changement.
3	Modéré	Le risque est gérable et ne peut pas corrompre significativement l'entreprise à long terme. Dois être traité et atténué. L'atténuation à tout prix pourrait ne pas être abordable.
4	Critique	Des mesures doivent être évaluées à court terme. Des mesures partielles doivent être mises en place comme solution rapide. Ce risque est suivi et examiné aux réunions SCI. Il fait partie du rapport annuel au conseil. Des mesures sont revues au moins 1 fois par an. Tout nouveau risque identifié doit avoir un responsable de défini qui réalise un suivi. Importance 4.
5	Catastrophique	Des mesures doivent être évaluées à court terme. Des mesures partielles ou suivies doivent être mises en place comme solution rapide. Ce risque est suivi et examiné aux réunions SCI. Il fait partie du rapport annuel au conseil. Des mesures sont revues au moins 2 fois par an. Tout nouveau risque doit avoir un responsable et peut-être un groupe de travail doit être élu et réaliser un suivi. Importance=5.

Le 2ème tableau définit les termes utilisés quant à la probabilité d'un évènement se produise ou non. J'ai utilisé le même système de graduation que le tableau 1. Au niveau 1 nous avons un évènement qui a une chance de se produire hautement improbable, alors qu'en 5, il s'agit d'un évènement qui peut se produire plusieurs fois par an.

Tableau XVIII : Niveau de probabilité/Récurrence

		Probabilité : Combien de fois un risque peut se produire
1	Improbable	Ne se produit jamais ou très rarement
2	Rare	Moins de 1 fois par an
3	Occasionnel	Environ 2 à 3 fois par an
4	Probable	Environ 3 à 4 fois par an
5	Fréquent	Environ 5 fois et plus par an

Le 3ème tableau définit quel impact peut avoir un évènement sur le groupe, toujours avec la même échelle de graduation : le niveau le plus bas (1) aura un impact négligeable alors que le niveau le plus élevé aura un impact catastrophique.

Tableau XIV : Niveau d'impact

1	Négligeable	Pas d'impact significatif
2	Bas	Le risque a un impact sur l'entreprise, mais il est atténué par des mesures efficaces comme le workflow dans les applications, des processus clairs et de la formation.
3	Modéré	Le risque a un impact significatif et n'a pas encore été atténué par les mesures. Il peut être géré en dehors des COPILs.
4	Critique	Le risque a un impact significatif sur un ou plusieurs aspects, généralement sans impact sur la stratégie. Cependant, il doit être traité avec diligence dans un délai approprié : · Escaladé au COPILs, car il nécessite une décision de gestion. · Les mesures prises pour réduire les risques. · Si le risque ne peut être réduit de manière significative, alors une « mesure spécifique de contrôle » doit être documentée et le risque suivi dans le site intranet SCI. L'évolution du risque doit être évaluée régulièrement.
5	Catastrophique	A un impact majeur sur un ou plusieurs aspects, y compris la stratégie. Ce risque doit être traité en priorité. · Escaladé au COPILs, car il nécessite une décision de gestion. · Les mesures prises pour réduire les risques. · Si le risque ne peut être réduit de manière significative, alors une « mesure spécifique de contrôle » doit être documentée et le risque suivit dans le site intranet SCI. L'évolution du risque doit être évaluée régulièrement par le SCI.

La synthèse de ces 3 tableaux donne un tableau croisé final, appelé tableau de synthèse. Dans ce tableau, nous retrouvons en ordonné le niveau d'impact gradué de 1 à 5, en abscisse la probabilité graduée aussi de 1 à 5 et dans chaque cellule, la valeur du croisement des deux données.

Il faut donc lire le tableau comme ceci : pour les case[a] et case[b] :

Quelle est la valeur toujours graduée de 1 à 5 pour qu'un évènement improbable et ayant un impact catastrophique sur le groupe se produise, 2 sur 5. Ou alors quelle valeur peut avoir un évènement qui se produit fréquemment et qui a un impact critique sur le groupe, 5 sur 5.

Tableau XX : Tableau de synthèse

		Récurrence/Probabilité				
		Improbable (1)	Rare (2)	Occasionnel (3)	Probable (4)	Fréquent (5)
Impact	Catastrophique (5)	case[a] 2	3	5	5	5
	Citrique (4)	2	3	4	4	case[b] 5
	Modéré (3)	2	2	2	2	4
	Faible (2)	1	1	2	2	2
	Négligeable (1)	1	1	1	1	1

Lors de l'analyse suivante avec l'analyse des risques, les scénarios de crise retenus sont ceux ayant une valeur estimée dans le tableau de synthèse égale ou supérieure à 3 et un impact financier moyen, élevé ou critique.

2.2.2 Identification des applications essentielles à l'activité du groupe

Dans le cadre d'une société de service informatique, les moyens logistiques et techniques permettant la réalisation des processus métiers sont identifiés comme étant les applications et par déduction, les moyens matériels sur lesquels s'appuient les applications pour fournir les services aux différents métiers de l'entreprise. L'étape suivante a donc été de cartographier les applications informatiques, serveurs, base de données et éléments réseaux, liés aux activités des services et jugés comme critiques dans la 1ère partie.

2.2.2.1 Cartographie des applications informatiques

Cartographie Lotus Notes

L'infrastructure Lotus Notes (*Fig VII. Cartographie infrastructure Lotus Notes)* permets l'accès à toutes les informations Ressources Humaines propres à chaque collaborateur (*Informations personnelles, CV, formation, gestion des congés, rapport des revues annuelles*) ainsi qu'à une partie planning et gestion/facturation des projets. Elle est composée d'un serveur de production, d'un serveur de sauvegarde où toutes les bases Lotus Notes sont dupliquées, d'un serveur de développement de base et d'un serveur d'archivage des anciennes boîtes mails. Un serveur relais est installé en zone démilitarisée (DMZ) pour jouer le rôle de passerelle depuis l'extérieur.

Tous ces serveurs sont sauvegardés quotidiennement (*point Mode de récupération et type de sauvegarde actuel*).

Le service Lotus Notes est assuré sur l'infrastructure DC uniquement.

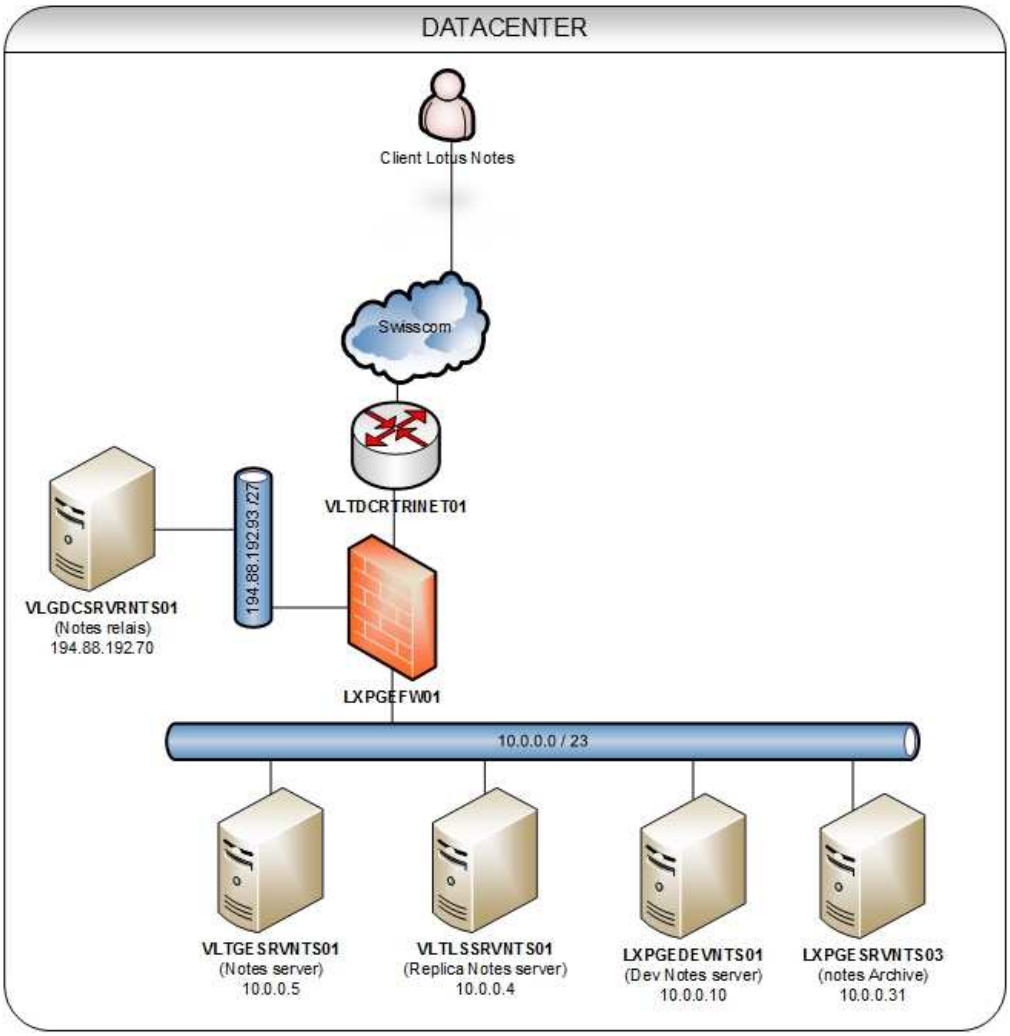


Fig. VII : Cartographie infrastructure Lotus Notes

VLTGESRVNTS01 est le serveur de production, le serveur VLTLSSRVNTS01 est le serveur de sauvegarde où toutes les bases Lotus Notes sont dupliquées. Le serveur LXPGEDEVNTS01 est dédié pour le développement et le serveur LXPGESRVNTS03 joue le rôle de base d'archivage des anciennes boîtes mails. Un serveur relais VLGDCSRVRNTS01 est installé en DMZ pour jouer le rôle de passerelle.

Cartographie ERP Microsoft Dynamics Navision

L'infrastructure de progiciel de gestion intégré (PGI) (*Fig VIII. Cartographie infrastructure Microsoft Dynamics Navision*) plus communément appelé Enterprise Resource Planning (*ERP*) Microsoft Dynamics Navision est composée de 2 serveurs. Un serveur de production un serveur de bases de données SQL (*Microsoft SQL*) qui héberge l'ensemble des bases de données (*Production et Test*).

L'ERP est accessible uniquement par la ferme de serveurs Citrix et le service est hébergé sur le Datacenter. Il n'existe pas d'infrastructure de backup/DRP.

Ces deux serveurs sont sauvegardés quotidiennement (*point Mode de récupération et type de sauvegarde actuel*).

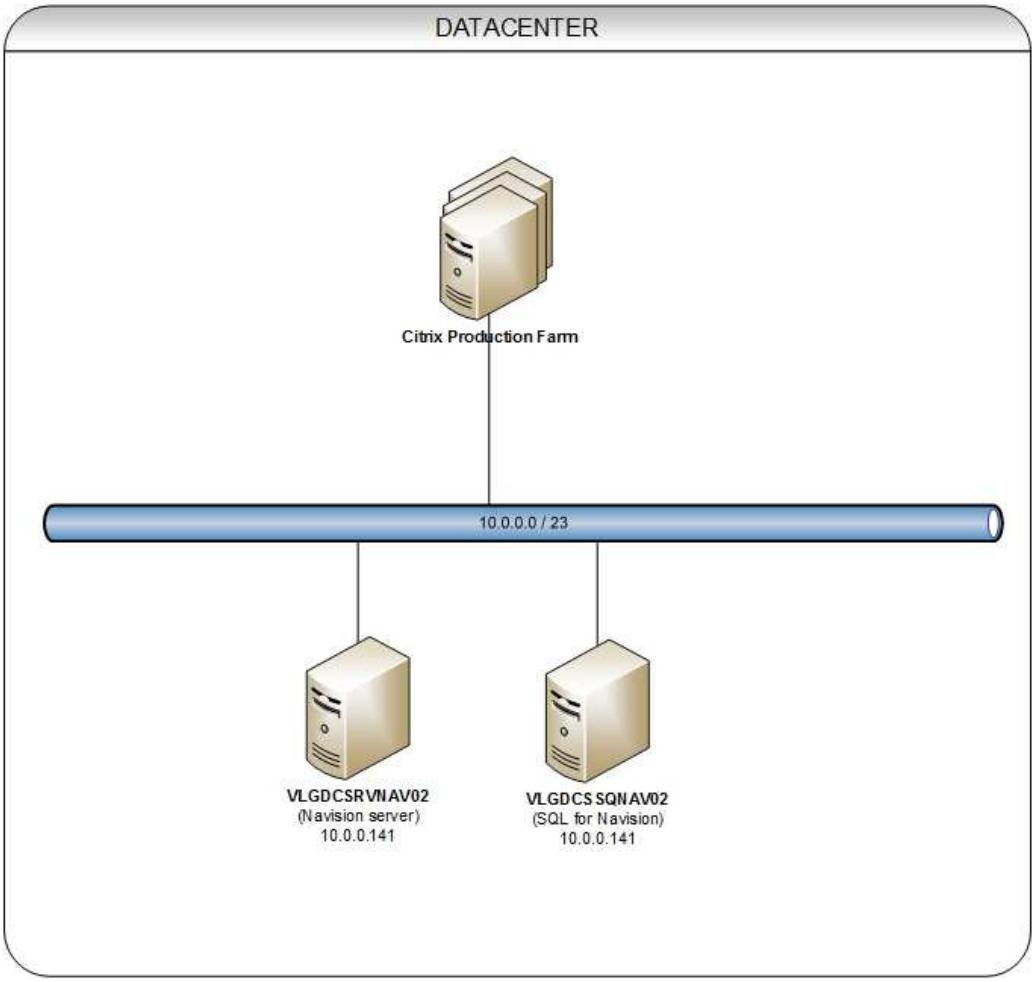


Fig. VIII : Cartographie infrastructure Microsoft Dynamics Navision

L'infrastructure de l'ERP Microsoft Dynamics Navision est composée de 2 serveurs. Un serveur de production VLGDCSRVNAV02 et d'un serveur SQL (Microsoft SQL) VLGDCSSQNAV02 qui héberge l'ensemble des bases de données (Production et QA(Développement)).

Cartographie Messagerie et accès distant (Microsoft TMG)

L'infrastructure de messagerie (*Fig. IX Cartographie infrastructure Messagerie et Remote access*) est assurée par les éléments suivants :

Un serveur Microsoft Exchange dans le Datacenter qui héberge l'ensemble de rôles dévolu à un serveur de messagerie (*hébergement des boites mails, distribution du courrier, etc.*) et un serveur Microsoft Exchange dans le Datarecovery avec les mêmes rôles. Les serveurs sont configurés dans un mode Microsoft failover Cluster qui permet le basculement automatique des bases d'un site sur l'autre en cas de défaillance.

L'infrastructure Datacenter héberge aussi un serveur Cisco Ironport qui joue le rôle de passerelle et qui permet donc l'échange du courrier informatique avec l'extérieur du groupe.

Un serveur installé avec les fonctionnalités Microsoft TMG (*Threat Management Gateway*) joue le rôle de proxy inversé (*reverse proxy*) pour la configuration automatique des clients Outlook qui utilisent la technologie de découverte automatique (*autodiscover*). Cette technologie permet la configuration automatique des clients de messagerie depuis l'intérieur ou l'extérieur du groupe.

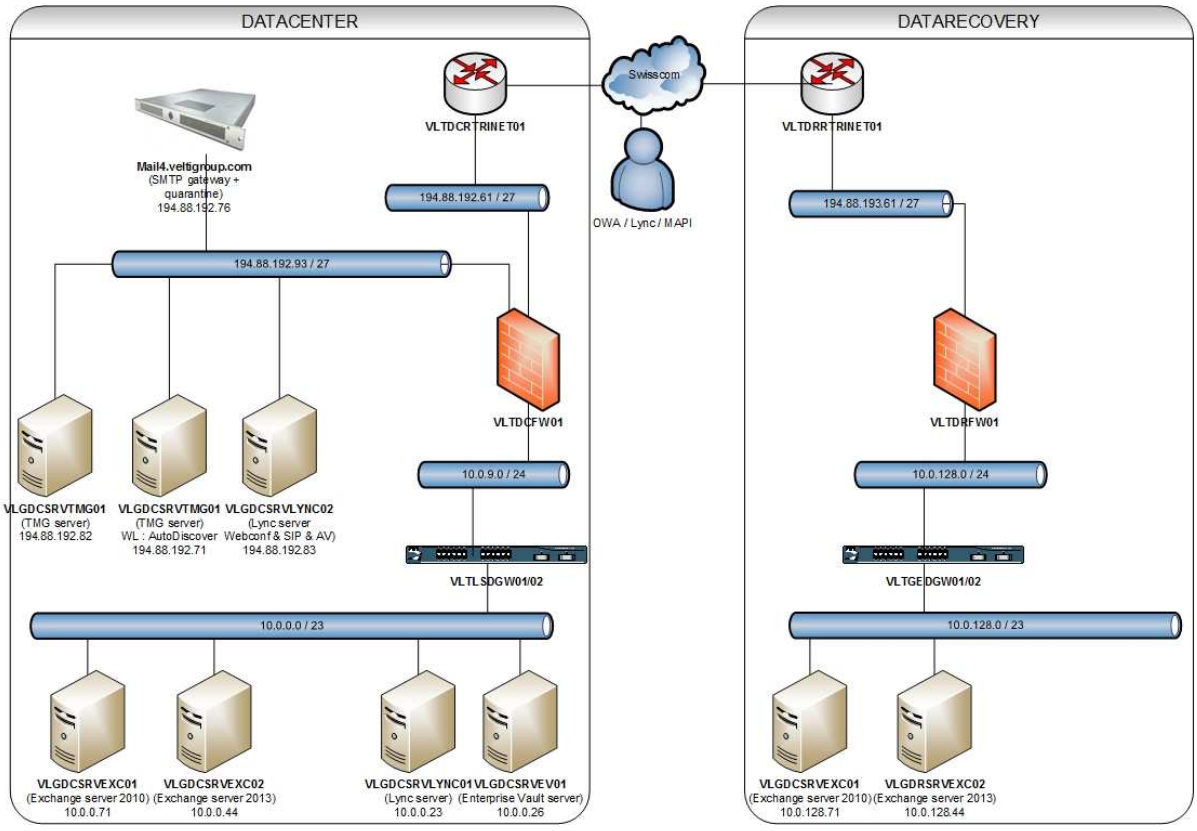


Fig. IX : Cartographie infrastructure Messagerie et Remote access

L'infrastructure de messagerie est assurée par les éléments suivants :

Un serveur Microsoft Exchange dans le Datacenter (VLGDCSRVEXC01) et un serveur dans le Datarecovery (VLGDRSRVEXC01), les serveurs sont configurés avec un mode Microsoft failover Cluster qui permet le basculement des bases automatique d'un site sur l'autre.
Une passerelle Cisco Ironport (mail4.veltigroup.com) est située dans le Datacenter.

Un serveur Microsoft TMG (VLGDCSRVTMG01) qui joue le rôle de reverse proxy pour la configuration automatique des clients Outlook (autodiscover).

Cartographie Citrix

L'ensemble des services transverses du groupe utilise une infrastructure virtuelle basée sur les produits des marques VMware et Citrix. Les applications métiers (*Ressources Humaines, Comptabilité, Administration*) ne sont accessibles que depuis ces infrastructures. Il n'y a actuellement pas de redondance de services à ce niveau.

L'infrastructure Citrix est donc composée des éléments suivants (*Fig X. Cartographie infrastructure Citrix*):

- 7 serveurs de production pour l'utilisation de bureaux virtuels,
- 2 serveurs de management pour le service support client,
- 1 serveur de management pour le service VIT,
- 1 serveur Citrix Storefront qui fournit les interfaces de service,
- 1 serveur Microsoft SQL,
- 1 serveur Xendesktop qui délivre les applications et les bureaux virtuels,
- 1 serveur de licences.

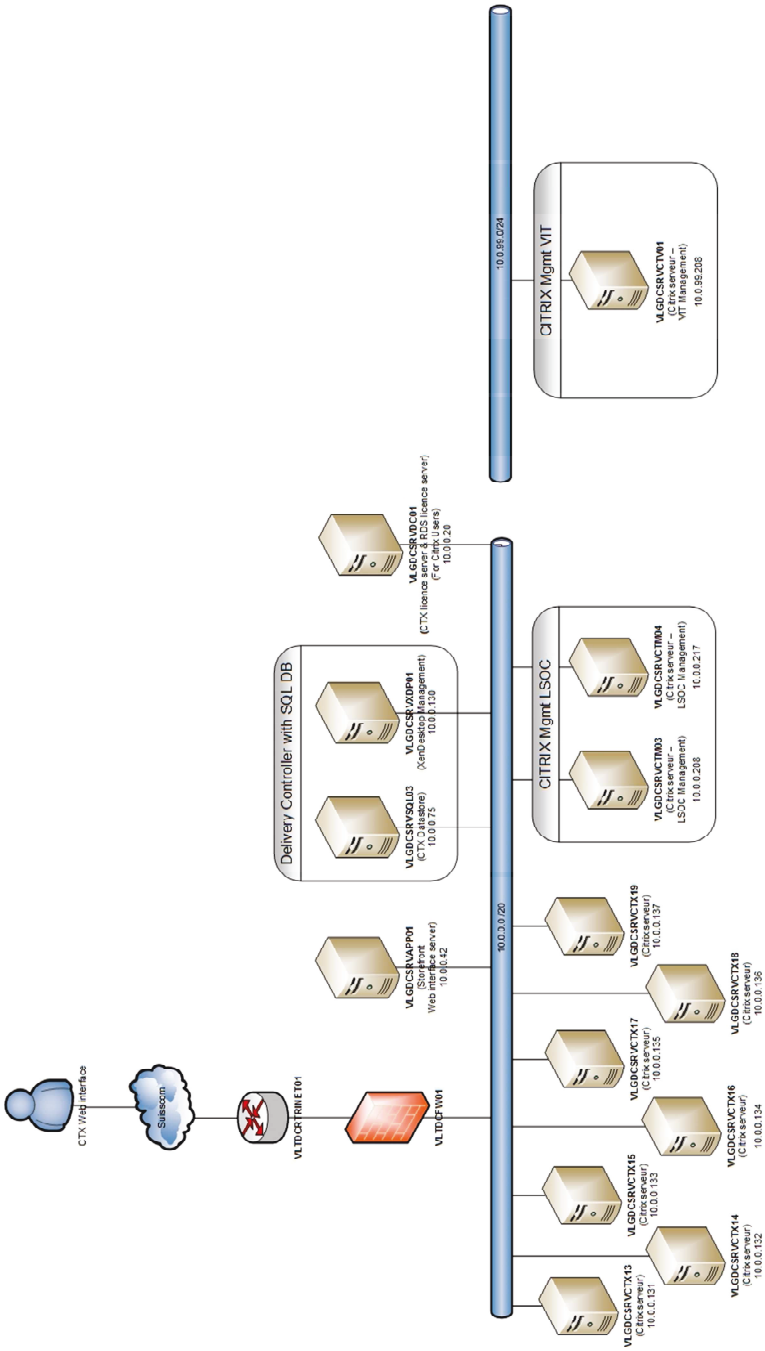


Fig. X : Cartographie infrastructure Citrix

L'infrastructure Citrix est composée des éléments suivants :

- 7 serveurs de production VLGDCSRVCTX13 à VLGDCSRVCTX19,
- 2 serveurs de management support VLGDCSRVCTM03 et VLGDCSRVCTM04,
- 1 serveur de management VIT - VLGDCSRVCTV01,
- 1 serveur Citrix Storefront qui fournit les interfaces de service - VLGDCSRVAPP01,
- 1 serveur Microsoft SQL - VLGDCSRVSQL03,
- 1 serveur Xendesktop qui délivre les applications et les bureaux virtuels - VLGDCSRVXDP01,
- 1 serveur de licences.

Cartographie Intranet

L'intranet du groupe est développé sur le produit Microsoft SharePoint (*Fig XI. Cartographie infrastructure Intranet*). Il n'y a pour le moment pas de redondance des infrastructures pour ce service. L'intranet héberge toutes les informations du groupe et est structuré par société. Il permet, via une gestion fine des droits en lecture et écriture, l'accès à toutes les procédures informatiques ainsi qu'à toutes les informations concernant les clients, contrats, partenariats, etc.
Le service Intranet du groupe est assuré par 3 serveurs Microsoft Windows :

- 1 serveur Microsoft Sharepoint,
- 1 serveur Microsoft SQL,
- 1 serveur Frontal (Front End).

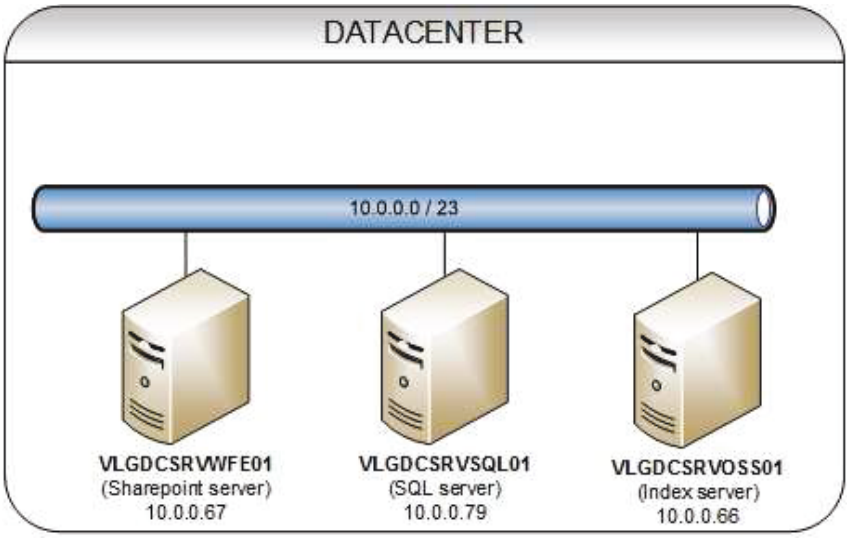


Fig. XI : Cartographie infrastructure Intranet

Le service Intranet du groupe est assuré par les 3 serveurs Microsoft Windows suivants :

- 1 serveur Microsoft Sharepoint - VLGDCSRVOSS01,
- 1 serveur Microsoft SQL - VLGDCSRCSQL01,
- 1 serveur Front End - VLGDCSRVWFE01.

Cartographie EasyVista

Actuellement le service de ticketing du support client et de l'IT interne est fourni par l'infrastructure EasyVista (*Fig XII.Cartographie infrastructure Ticketing*), nom du logiciel développé par cette même société, qui se situe dans le Datacenter. Cette infrastructure est accessible depuis l'internet pour permettre aux clients du groupe un suivi de leur ticket ouvert auprès du service de support.

Elle est composée :

- 1 serveur de production, applicatif,
- 1 serveur web – apache,
- 1 serveur Active Directory LDS pour l'authentification externe,
- 1 serveur SQL.

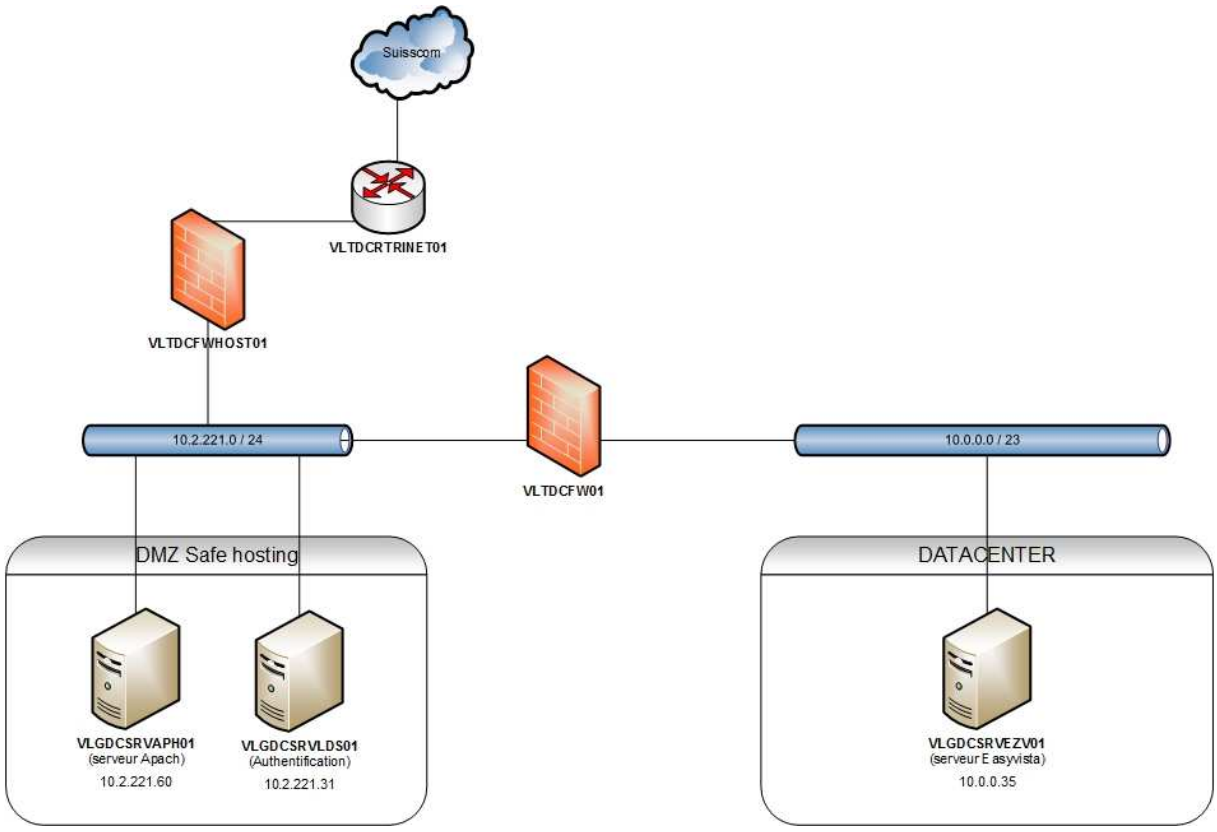


Fig. XII : Cartographie infrastructure Ticketing

Le service de ticketing du support client et de l'IT interne est fourni par l'infrastructure EasyVista, qui est composée :

— un serveur de production, applicatif - VLGDCSRVEZV01,
— un serveur web – apache - VLGDCSRVAPH01,
— un serveur Active Directory LDS pour l'authentification externe - VLGDCSRVLDS01.

Cartographie Téléphonie

L'infrastructure téléphonique est aujourd'hui assurée par quatre matériels de la marque Cisco (*Fig. XIII Cartographie infrastructure Téléphonie*). Ces matériels permettent la gestion des appels internes et externes, mais aussi la gestion des appels vers les services supports informatiques internes (*VIT*) et supports clients. Ils prennent donc en charge, les files d'attente, l'enregistrement des appels et quantité d'autres services dédiés aux centrales d'appel.

L'infrastructure est composée des éléments suivants :

- 1 PABX,
- 1 serveur Call Manager,
- 1 serveur de Présence,
- 1 serveur (*voiceMail*) pour l'enregistrement des messages vocaux,
- 1 serveur appelé Call Center dédié à la gestion des services supports.

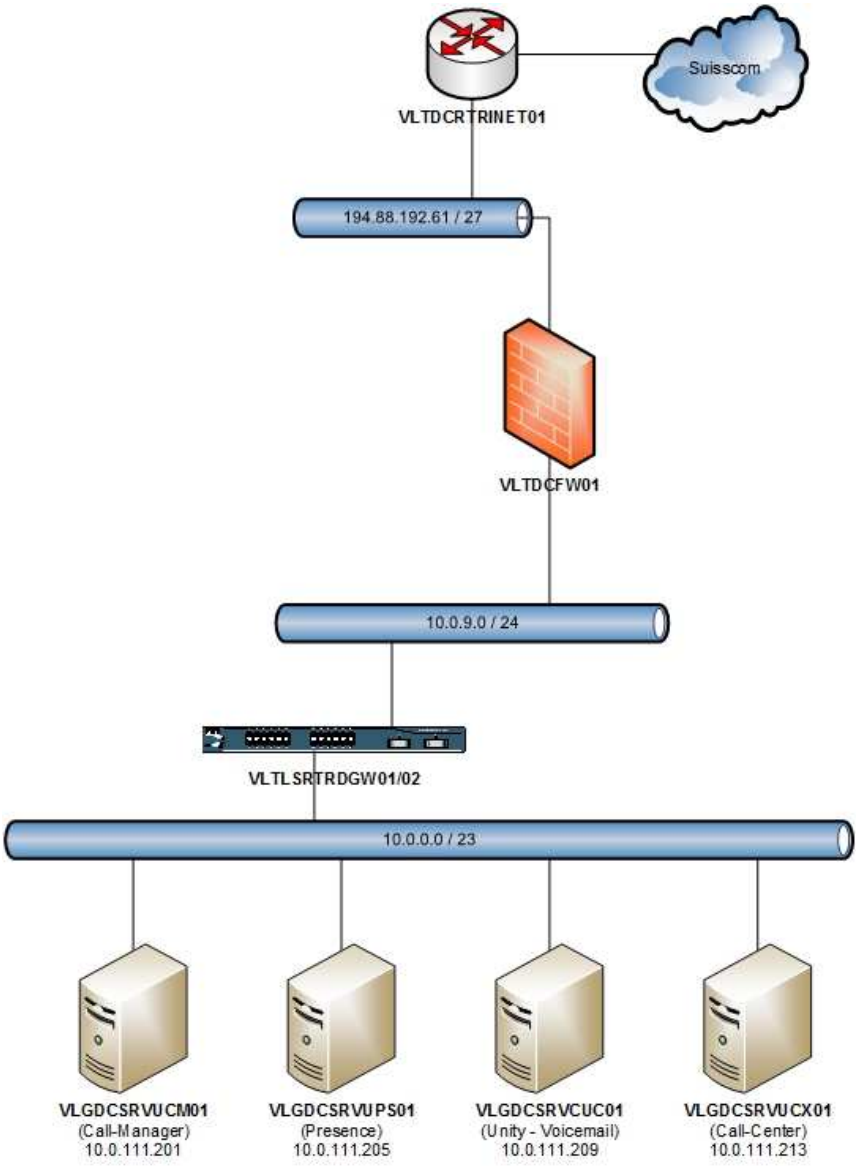


Fig. XIII : Cartographie infrastructure Téléphonie

L'infrastructure est donc composée des éléments suivants :

- 1 PABX que l'on nomme aussi routeur voix – VLTLSRTRDGW01,
- 1 serveur Call Manager – VLGDCSRVUCM01,
- 1 serveur de Présence – VLGDCSRVUPS01,
- 1 serveur (*voiceMail*) pour l'enregistrement des messages vocaux – VLGDCSRVCUC01,
- 1 serveur appelé Call Center dédié à la gestion des services supports – VLGDCSRVUCX01.

2.2.2.2 Analyse des risques, Identification des différents types de menaces

L'étape suivante consiste à lister l'ensemble des risques et menaces auxquels sont soumis le groupe et les services informatiques. En nous basant sur les tableaux de l'étape précédente (*tableau d'importance, d'impact, de probabilité/récurrence et de synthèse*) nous avons attribué une valeur de 1 à 5 à chacun des risques. C'est à partir de cette étape que j'ai pu déterminer et faire valider dans quel cas il avait nécessité d'assurer un service de continuité et pour quelles applications/services.

Tableau XXI : Liste des différents risques auxquels est soumis le groupe

Risques Physiques	*Description*	*Valeur Tableau Synthèse*
Dégât des eaux, crues :	Destruction totale ou partielle des locaux ou équipements (ex : foudre)	2
Pollution :	Présence de vapeur, de gaz corrosif ou toxique	2
Accidents majeurs :	Explosion de sites industriels, accident d'avion	2
Incendie :	Destruction totale ou partielle d'équipements	3*

Naturels

Phénomène climatique :	Conditions extrêmes de chaleur et de froid	2
Phénomène sismique, volcanique :	Zone à risque	2
Phénomène météorologique :	Tempêtes, ouragans, pluies de grêle	2

Perte de services essentiels

Défaillance de la climatisation :	Son arrêt peut provoquer le dysfonctionnement ou l'arrêt du SI	3
Perte d'alimentation énergétique :	Fermeture du fournisseur d'électricité	3
Perte des télécommunications :	Absence de réseau téléphonique	3

Rayonnements

Rayonnements électromagnétiques, thermiques :	Radar, antenne radio, rayonnements, etc. (micro coupures)	2

Défaillance technique

Panne matérielle :	Usure, vieillissement, défaut de maintenance, mauvais emploi	2
Dysfonctionnement matériel :	Dégradations, erreurs de programmation…	2
Saturation du matériel :	Engorgement, dépassement calcul, stockage, requêtes…	2
Dysfonctionnement logiciel :	Mauvaise conception, installation, modifications du logiciel	2
Atteinte à la maintenabilité du SI :	Pb fournisseurs, pb administratif (séquestre des programmes sources)	2

Agression physique, Erreur, Mouvement Social

Destruction des matériels :	Ex : sabotage des supports de données	1
Reniement d'actions :	Id répudiation = négation de participation à un échange d'informations	1
Erreur de saisie :	Ex : données fausses	3
Erreur d'utilisation :	Manipulation, utilisation matériels, virus…	3
Grève	Ex. Grève des transports ou mouvement social	3

Crise Sanitaire, pandémie

Crise sanitaire :	Virus, pandémie, épidémie, maladie contagieuse	3

Crise Informatique

Attaque, Virus	Attaque informatique, virus	3

Compromission des informations et des fonctions

Interception de signaux parasites compromettants :	Possibilité de se connecter aux câblages, tuyauteries, etc.	2
Espionnage à distance/Écoute passive :	Surveillance de l'activité (câble, réseau…	2
Vol de supports ou de documents :	Vol de supports magnétiques ou papier	2
Effraction/Vol de matériels :	Micro-ordinateurs, modems, etc.	4
Divulgation interne/externe :	Accidentelle ou intentionnelle (téléphone télécopie, messagerie.)	2
Informations sans garantie d'origine :	Faux ou contrefaçons (atteinte fiabilité des informations)	2
Piégeage du matériel :	Pour permettre l'interception et la transmission d'informations	2
Utilisation illicite du matériel :	Pour bénéficier des services rendus par le système	2

Compromission des informations et des fonctions (suite)

Piégeage du logiciel :	Fonctions cachées (virus, cheval de Troie, trappe, canal caché.)	2
Abus de droit :	Ex-administrateur réseau qui modifie les caractéristiques d'exploitation	2
Usurpation de droit :	Usurpation d'identité/substitution (interception//connexion)	2
Fraude :	Monétaire/Ex : utilisation codes carte bleue	3
Altération du logiciel :	Action visant à altérer ou détruire les programmes (ex : bombe logique)	2
Copie frauduleuse du logiciel :	Copies pirates par le personnel	4
Utilisation de logiciels contrefaits ou copiés		4
Altération des données :	Interception avec modification, balayage (numéros d'accès), virus	2
Atteinte à la disponibilité du personnel :	Maladie ou tout empêchement, volontaire (absentéisme…)	2

2.2.3 Solutions testées et retenues

La direction a souhaité que j'étudie deux possibilités :

1. Soit une offre de cloud dédiée qui est proposée par une société du groupe, Exoscale (*spin-off*).

Cette société nous offre la possibilité de déployer des services au sein de leurs infrastructures informatiques, situées dans un Datacenter dans le centre de Genève. Cette solution offre des avantages et inconvénients que j'ai listé et que j'ai présenté lors de l'exposé du choix de la solution retenue.

Avantages : Image du groupe, aide à la promotion des produits Exoscale, rabais facturation pour Veltigroup, données géolocalisées en Suisse, pas de gestion des infrastructures d'hébergements des services.

Inconvénients : Facturation compliquée (*Veltigroup doit réimputer aux sociétés du groupe propriétaires des serveurs*), tarifs élevés, car calculés au temps de fonctionnement des serveurs. Ajout d'un VPN permanent entre les infrastructures Exoscale et Veltigroup pour les services en cluster ou de basculement. Monitoring moins réactif, car non géré directement par le VIT.

2. Soit un upgrade de l'infrastructure Datarecovery (*DR*) de Genève afin que celle-ci puisse supporter un arrêt complet de l'infrastructure du Datacenter (*DC*), soit environ 150 serveurs virtuels.

Avantages : Le Veltigroup IT (VIT) surveille (*monitore*) ses propres infrastructures, tous les projets sont gérés par le VIT : (*déploiement des machines, installation des systèmes d'exploitation*), expérience acquise pour les ingénieurs du VIT, de nouveaux projets concomitants peuvent être étudiés (*exemple : Upgrade de l'infrastructure messagerie vers des Appliance en mode cluster*).

Inconvénients : Investissement conséquent.

1er cas : L'offre de Cloud dédié

Deux paramètres ont été pris en compte : technique et financier. Au niveau technique nous avons les contraintes de service en Haute Disponibilité (*HA*) avec par exemple, le service de messagerie Exchange en Cluster. Il faut donc maîtriser l'adressage réseau Exoscale qui nous est dédié pour pouvoir implémenter certains services. Il nous faut aussi pouvoir surveiller activement (*monitorer*) les serveurs et les services.

Pour répondre à ces questions, il a donc été décidé de réaliser un test de faisabilité (*POC, Proof Of Concept*).
Schématiquement, un Réseau Privé Virtuel (*VPN*) a été créé entre Exoscale et Veltigroup, un Virtual LAN (VLAN) a été dédié pour isoler le trafic entre les matériels qui le nécessitaient.

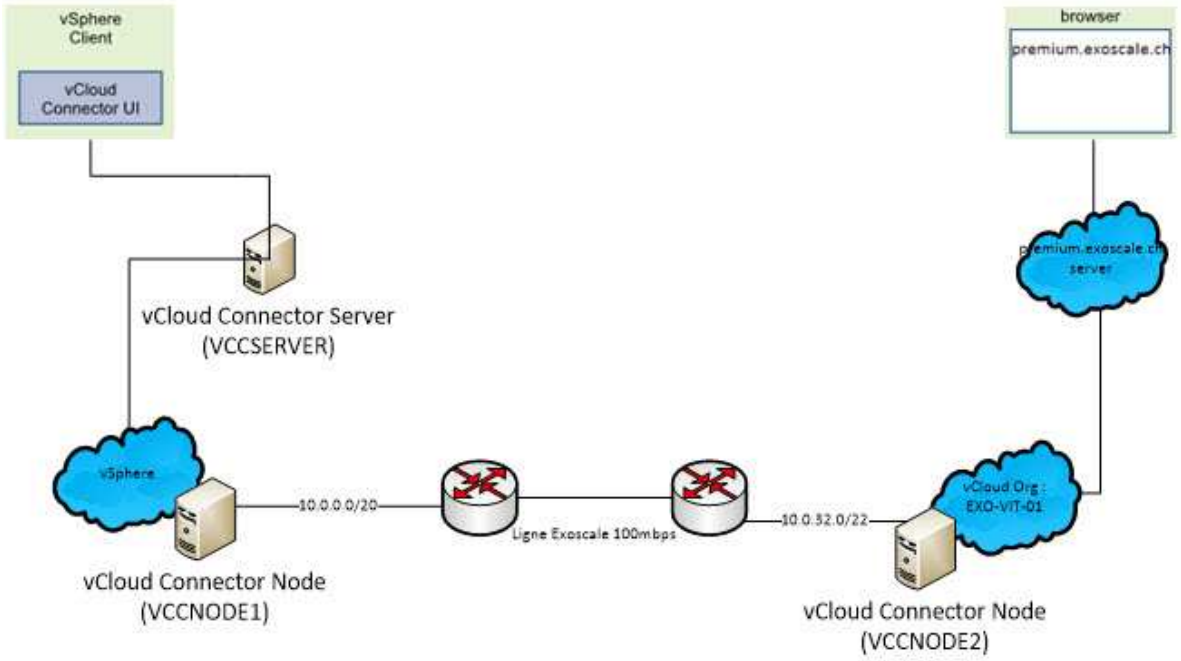


Fig XIV Synoptique Schéma réseaux (Veltigroup – Exoscale)

Cinq serveurs ont été déployés sur l'infrastructure Exoscale pour réaliser les tests.
Constat : Les machines sont difficilement gérables, il n'y a pas d'accès direct au système d'exploitation (RDP) seul un client Firefox v.29 permet de prendre la main sur la machine. Le déploiement des serveurs virtuels se fait via un système de transfert de fichiers ISO qui n'est aussi pas très ergonomique.
Si un serveur à un problème particulier, il est très difficile de connaître le statut exact de ce serveur.

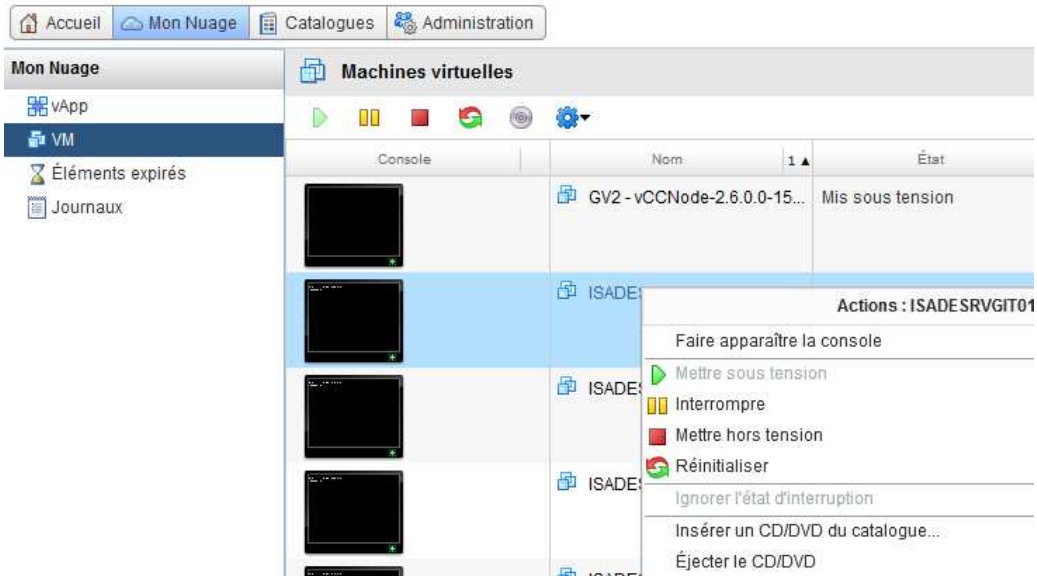


Fig. XV : Interface graphique de gestion des VM Serveurs sur Firefox v.29

Au niveau financier, le coût de fonctionnement de cinq serveurs sur un mois a été élevé (**1 400 CHF**). Le coût est calculé avec plusieurs paramètres (*CPU* + *Ram* + *Espace Disque SSD*) + Temps d'utilisation du serveur *(serveur allumé*). Sur ces cinq serveurs, un a été allumé en permanence (*Exchange – Service Cluster*) et quatre ont été allumés occasionnellement (*serveurs de développement*). Ce coût est à diviser et réimputer aux sociétés du groupe selon leur nombre de serveurs. La refacturation est compliquée car nous n'arrivons pas à avoir de détail pour chaque machine virtuelle.

2ème cas : Upgrade des infrastructures en place

Les deux mêmes paramètres ont été pris en compte, à savoir technique et financier.

Au niveau technique, il faut prévoir un upgrade de l'infrastructure de stockage et un upgrade de l'infrastructure de virtualisation. Le Datarecovery (*DR*) site est composé actuellement de 3 serveurs ESX Cisco UCSC, qui devra être amené à 5 serveurs pour supporter la charge processeur et mémoire. Le système de stockage, SAN (*Storage Area Network*) devra être changé, l'AMS 500 n'est plus maintenu par Hitachi, il sera remplacé par un EMC VNX5200 équivalent à celui du Datacenter.

Au niveau financier, l'investissement est assez conséquent : 2 serveurs CISCO UCSC-C240-M3L + baie EMC VNX5200 plus les ports fibres et les contrats de maintenance associés avec les rabais Veltigroup est de l'ordre de **20 000 CHF**.

Le choix de la Direction s'est porté sur cette possibilité, avec validation d'une durée des investissements de 3 ans au minimum.

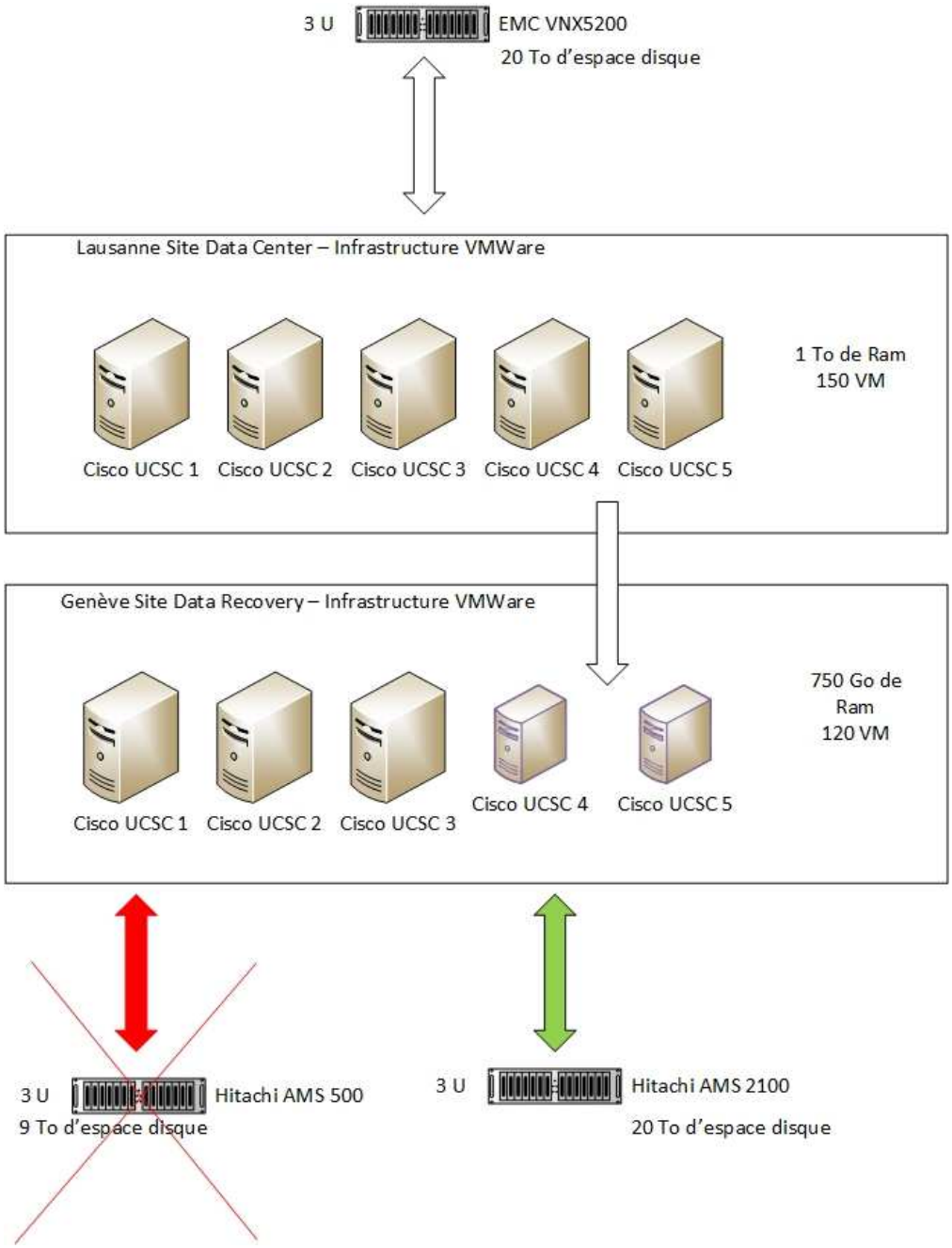


Fig. XVI Évolution du site DataRecovery par l'ajout de matériel

2.2.3.1 Technologies sélectionnées maîtrisées

Le groupe Veltigroup SA ayant pour cœur de métier les services informatiques, le groupe dispose des ingénieurs ayant les connaissances et compétences dans diverses technologies qui pourront être mises en œuvre. L'ensemble du système d'information est virtualisé par les produits VMware. La virtualisation est une technologie par laquelle un logiciel de virtualisation, simule une machine vis-à-vis d'un système d'exploitation. 5 serveurs Cisco ; appelés systèmes hôte supportent l'ensemble des serveurs virtualisés du Datacenter au niveau processeurs et mémoire. Le stockage des machines virtuelles est réalisé sur une baie de stockage de marque EMC VNX5200 disposant de 20 To d'espace disque.

Pour pouvoir assurer un maximum de disponibilité les solutions suivantes ont été sélectionnées.

Solutions haute-disponibilité :

- Cluster système,
- Cluster applicatif,
- Cluster d'équipements réseau.

Un cluster est une grappe de plusieurs serveurs, appelés nœuds, fonctionnant soit en parallèle pour équilibrer une charge de travail (*cluster actif-actif*), soit en secours pour assurer une meilleure continuité de service (*cluster actif-passif*). Dans les technologies que nous avons mises en œuvre le système de basculement sur un second serveur peut se réaliser de manière automatique ou manuellement.

Par exemple, pour sécuriser les bases de données SQL, nous avons utilisé la technologie Microsoft SQL Server AlwaysOn, qui est une nouvelle solution haute disponibilité et de récupération d'urgence dans SQL Server 2012.

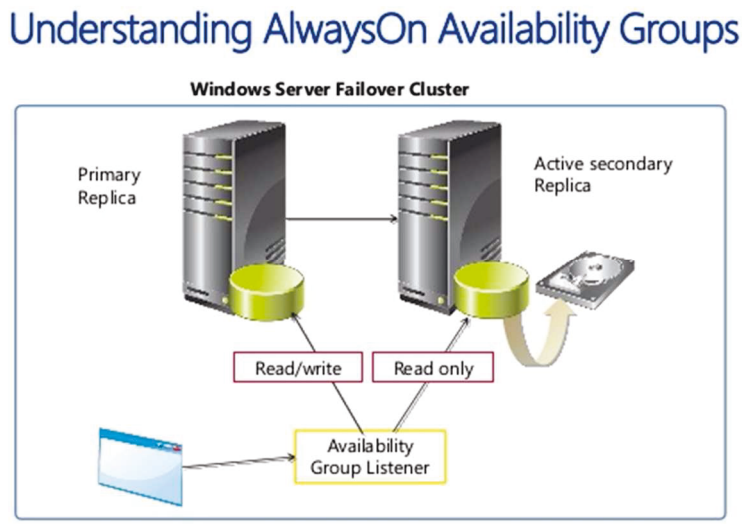


Fig. XVII : Technologie Microsoft AlwaysON

Cette solution permet par la mise en œuvre d'un ou plusieurs serveurs réplicas d'équilibrer la charge de travail en permettant l'accès aux bases de données en lecture simultané et permet aussi d'améliorer la résilience en permettant une bascule automatique en cas de défaillance.

Architecture sécurisée de réseaux multi-sites pour le transport et le stockage de données

- Design d'architecture de réseaux SAN Fibre Channel et iSCSI,
- Solutions d'interconnexion SAN longue distante : FC/IP, FC-FC, xWDM, partenariats opérateurs,
- Design d'architecture de réseaux LAN et WAN inter sites, VPN SSL, MPLS, etc.

Le site Datarecovery de Genève a donc été mise à jour avec des investissements conséquents dans un nouveau système de stockage, SAN de la marque EMC. La gestion de l'accès aux SAN est gérée via des commutateurs réseaux dédiés au stockage que l'on appelle Fabric (*switch dans la représentation ci-dessous*). Ces éléments permettent d'assurer un multiplexage et une redondance des accès aux éléments de stockage.

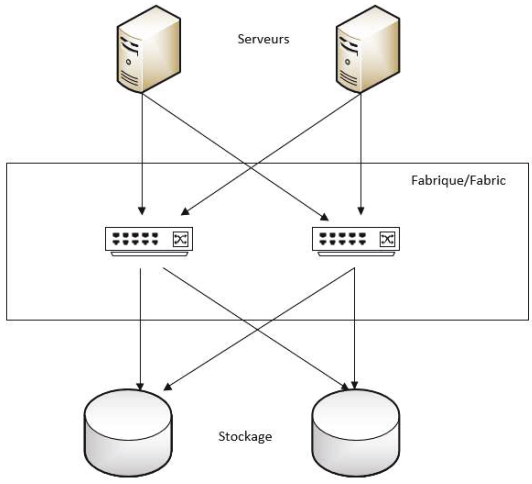


Fig. XIII : San Fabric communication

Au niveau réseau, il n'y a pas eu de modification à réaliser sur les différents éléments. Les protocoles réseau qui assurent une continuité de service comme Hot Standby Router Protocol (*HSRP*) sont déjà implémentés et les protocoles de gestion de route entre réseaux comme Border Gateway Protocol BGP sur internet sont aussi déjà optimisés.

Sécurisation et gestion du cycle des données

- Politique de sauvegarde, de restauration et d'externalisation des données (*multi supports*)
- Gestion des classes de stockage et archivage informatique

La sécurisation des données est assurée par des techniques et outils de sauvegarde qui sont développées au point suivant.

2.2.4 Définition des solutions de secours

2.2.4.1 Types de sauvegarde et Modes de récupération

L'utilisation des sauvegardes réalisées quotidiennement entre plus dans le cadre d'un Plan de Reprise d'Activité (*PRA*), mais peuvent aussi être utilisées lors de la phase de sortie de crise pour permettre la « reconstruction » d'une partie des infrastructures informatiques qui ont été détruites.

La préservation des données est réalisée par des sauvegardes quotidiennes différentielles et des mensuelles complètes. Les bandes sont stockées sur le site Datarecovery dans une armoire ignifugée. Il a été délibérément choisi d'éloigner les bandes du site Datacenter afin de disposer des sauvegardes intactes si le site de production principal était détruit ou endommagé. Pour pouvoir disposer d'une restauration rapide des informations, les premières sauvegardes sont réalisées sur le site de production et une opération de duplication des données est réalisée ultérieurement sur le site Datarecovery.

Toutes les procédures liées à l'utilisation de l'infrastructure de sauvegarde étaient existantes, la mise en place du système de sauvegarde a donné lieu à un projet à part entière, géré par un collaborateur du VIT. La fin du projet de sauvegarde s'est réalisée par l'écriture des procédures et la formation de tous les collaborateurs du VIT.

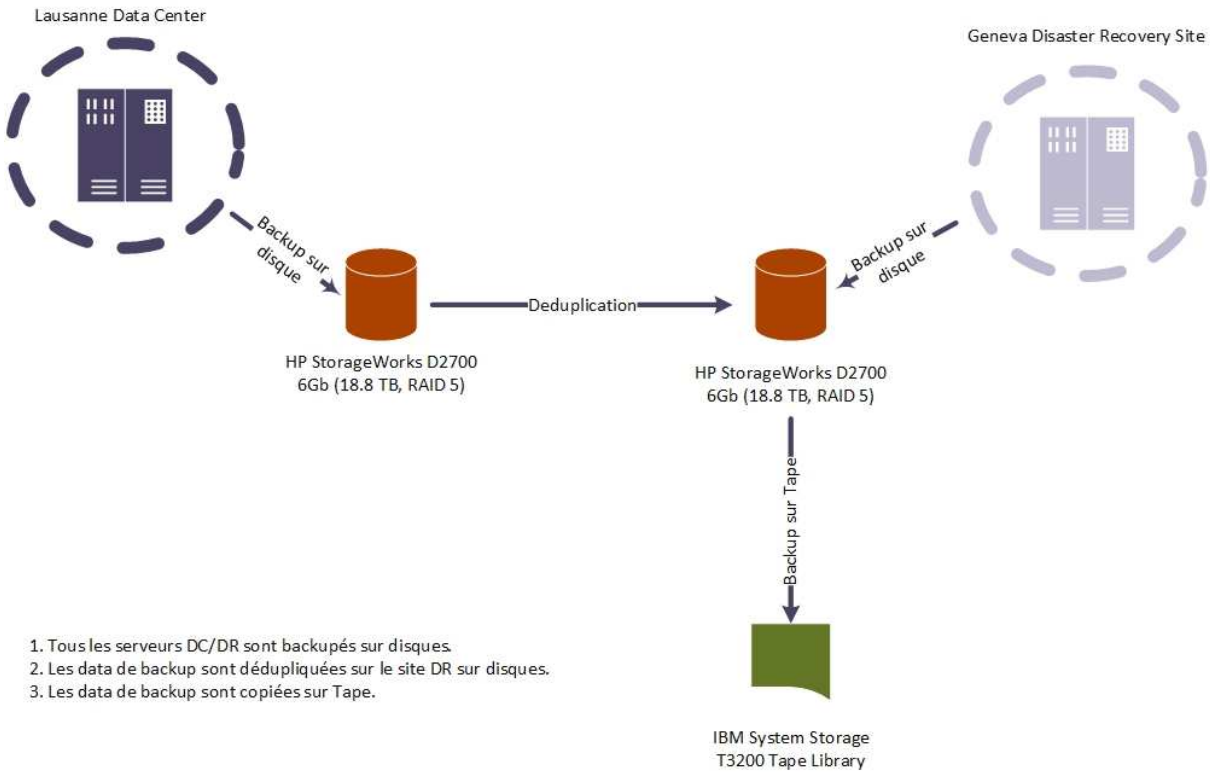


Fig. XIX : Représentation graphique du système de sauvegarde

Dans une première étape, pour les serveurs de Lausanne uniquement, les sauvegardes sont réalisées sur une baie de disque (*HP StorageWorks*). Les données sont ensuite dédupliquées sur le site de Genève et les sauvegardes des serveurs de Genève ont lieu.
Enfin, toutes les sauvegardes sont copiées sur des bandes qui se trouvent dans un robot de sauvegarde IBM System Storage. Une fois les sauvegardes finies, les bandes sont externalisées dans une armoire ignifugée.

Plusieurs politiques de sauvegarde existent et ces dernières se définissent par plusieurs paramètres : sauvegarde granulaire ou non, temps de rétention des données sur disques, sur bandes, etc.

Les sauvegardes des serveurs et des données sont réalisées selon trois fréquences : journalière, hebdomadaire et mensuelle. Des politiques de sauvegarde différentes liées aux types de services ont dû être définies. Par exemple des sauvegardes appelées granulaires pour les serveurs disposant de bases de données SQL. Les modes de sauvegardes sont ceux utilisés fréquemment, à savoir : sauvegarde complète et différentielle d'un serveur.

Tableau VI : Tableau des différents types de sauvegarde pour le site Datacenter

Site	Politiques	Fréquence	Sauvegarde Complète	Sauvegarde Différentielle
DC	**Serveurs Windows sans granularité**			
		Journalière		X
		Hebdomadaire	X	
		Mensuelle	X	
	Serveurs Windows avec granularité			
		Journalière		X
		Hebdomadaire	X	
		Mensuelle	X	
	Serveurs de messagerie Exchange – Bases actives			
		Journalière	X	
		Hebdomadaire	X	
		Mensuelle	X	
	Serveurs Sharepoint			
		Journalière	X	
		Hebdomadaire	X	
		Mensuelle	X	
	Serveurs Lotus Notes			
		Journalière		X
		Hebdomadaire	X	
		Mensuelle	X	
	Serveurs Entreprise Vault			
		Journalière	-	-
		Hebdomadaire	X	
		Mensuelle	X	

Tableau VII : Types de sauvegarde pour le site Datarecovery

Site	Politiques	Fréquence	Sauvegarde Complète	Sauvegarde Différentielle
DR	**Serveurs Windows sans granularité**			
		Journalière		X
		Hebdomadaire	X	
		Mensuelle	X	
	Serveurs Windows avec granularité			
		Journalière		X
		Hebdomadaire	X	
		Mensuelle	X	
	Serveurs de messagerie Exchange – Bases Actives			
		Journalière	X	
		Hebdomadaire	X	
		Mensuelle	X	

L'ensemble des procédures concernant l'outil de sauvegarde se trouvent sur l'intranet, département VIT. Un inventaire exhaustif des serveurs ainsi que toutes les informations relatives aux services hébergés sur ces serveurs sont maintenus à jour dans l'intranet. Cet inventaire permet d'avoir les informations minimales nécessaires lors d'intervention ou d'une réinstallation.

ITSDCSRVBCK99	Infrastructure	Server de Controle des Backups	other	LAN	DC	Warn GBA and PCO				
ITSDCSRVEXT01	Business Application	Extranet ITS	Windows 2008 R2	DMZ Hosting	DC	Outside working hours	ITSDCSRVSQL01	Cotting, Pierre		
ITSDCSRVEXT02	Business Application	Extranet ITS	Windows 2003	DMZ Hosting	DC	Outside working hours	ITSDCSRVSQL01	Cotting, Pierre		
ITSDCSRVKAS01	Business Application	Serveur Kaseya pour le support ITS	Windows 2008 R2	LAN	DC	Outside working hours - Attention pas de preinstallation dans la journée	ITSDCSRVSQL01	Cotting, Pierre		
ITSDCSRVKAS02	Business Application	Second serveur Kaseya ITS	Windows 2008 R2	DMZ Hosting	DC	Outside working hours, Warn ABC		Cotting, Pierre		
ITSDCSRVMGMT01	Management	Serveur de Management (demande GBA)	Windows 2012 R2	LAN	DC			Veltigroup Service Desk		
ITSDCSRVSEC02	Application delivery	Serveur Kaspersky en DMZ pour gérer les clients Kaspersky en interne et se connecter aux serveurs d'administration chez les clients ITS	Windows 2012 R2	DMZ Hosting	LS	Always		Veltigroup Service Desk	Demander à ITS pour la maintenance, si c'est bon pour eux il peut être redémarré à tous moments	

Fig. XX : Exemple page web liste des serveurs

2.2.4.2 Le Plan de Secours Informatique (PSI)

Le plan de secours informatique a été développé suite à la décision de la Direction du groupe lors d'un comité du Pilotage qui avait à l'ordre du jour le choix entre les deux types de solutions pour la continuité de l'activité. À savoir, travailler avec la société Exoscale et son offre de cloud dédié ou faire évoluer les infrastructures techniques du site Datarecovery donc de Genève pour qu'elles soient en phase avec les infrastructures du site Datacenter.

Lors de la présentation, tous les aspects importants ont été exposés. Les avantages et inconvénients des deux possibilités ont été développés, autant sur les aspects techniques que financiers.

Le choix de la direction s'est finalement porté sur l'évolution des infrastructures du site Datarecovery.

La réalisation du Plan de Secours Informatique a donc dans un premier temps donné lieu à la création de plusieurs sous-projets. Chaque sous-projet représentant une évolution à apporter en termes de service et/ou d'infrastructure au site Datarecovery.

Les sous-projets ont ensuite été affectés à chaque membre du département VIT.

Le Plan de Secours Informatique reprend donc pour chaque service la description détaillée des infrastructures en place sur les deux sites, Datacenter et Datarecovery, ainsi que les liens vers toutes les procédures et documentations liées à l'exploitation de ces services (procédures de basculement des services par exemple.

De plus, les tâches opérationnelles affectées au département VIT sont listées ainsi que la toute la documentation y faisant référence.

Toutes les décisions, quant aux évolutions techniques à apporter à chaque infrastructure, ont été prises en y associant les services qui utilisent les applications lors de groupe de travail. En associant l'ensemble des utilisateurs à ces multiples projets, on est arrivé à créer une adhésion assez générale avec des personnes moins réfractaires aux changements.

Les modifications suivantes ont donc pu être apportées aux infrastructures :

Cartographie Lotus Notes (*Annexe 6*)

L'infrastructure Lotus Notes a été complétée avec l'ajout d'un serveur relais dans la zone démilitarisée du site Datarecovery (*DMZ DR*) et d'un serveur de production dans le réseau de production. Le projet a été entièrement réalisé par le VIT. Il n'y a pas de procédure de basculement automatique sur l'infrastructure de DR. L'utilisation de l'infrastructure Lotus Notes DR se fait par la configuration du client Notes. La procédure de configuration du client Notes existante, qui est utilisée lors de la configuration des nouveaux embauchés, a été mise à jour avec la création du document site DR.

La procédure pour configurer le client lotus notes se trouve dans l'intranet, département VIT et il n'y a pas eu de nécessité de créer des tâches opérationnelles supplémentaires.

Cartographie ERP Microsoft Dynamics Navision (*Annexe 6*)

L'infrastructure de l'ERP Microsoft Dynamics Navision a été complétée dans le site DR avec l'ajout de 3 serveurs Citrix de production ainsi qu'un serveur Microsoft SQL et de la technologie SQL AlwaysOn. SQL Server AlwaysOn est une nouvelle solution Microsoft haute disponibilité et de récupération d'urgence dans SQL Server 2012.

La procédure de basculement sur l'infrastructure DR se fait de façon automatique, il n'y a donc pas de procédure associée. La création de plusieurs tâches opérationnelles a été nécessaire.

- Quotidienne : Vérification de l'état du Failover Cluster,
- Quotidienne : Vérification de l'état des bases SQL et de la technologie Always on.

Cartographie Messagerie et Remote access (TMG) (*Annexe 6*)

L'infrastructure de messagerie et d'accès à distance a été modifiée de deux manières :

Le remplacement du serveur physique Cisco Ironport qui avait la fonction de passerelle courrier pour les serveurs Microsoft Exchange, par deux Appliance Cisco Ironport, une se situant dans le Datacenter et l'autre dans le Datarecovery. Ces deux Appliance ont été configurées en mode cluster pour permettre une meilleure résilience. Il n'y a pas de procédure liée au fonctionnement du cluster, l'ensemble de la procédure se faisant de manière automatique.

L'ajout d'un serveur dans la partie démilitarisée Datarecovery (*DMZ DR*). Ce serveur est installé avec le produit Microsoft TMG.

La procédure de basculement manuel se trouve sur l'intranet, département VIT

Nouvelle Cartographie Citrix (*Annexe 6*)

L'ensemble de l'infrastructure Citrix existante est dupliqué sur le site Datarecovery.

Trois serveurs de production sont installés. Le système d'exploitation est maintenu à jour lors des journées patching par le VIT. Le serveur Storefront (*nouveau web interface*) est dupliqué sur le site Datarecovery également, il contient l'ensemble des profils utilisateurs Windows qui sont dupliqués via la technologie DFS-R de Microsoft.

Un serveur SQL est configuré avec la technologie Microsoft SQL AlwaysOn (*Failover Cluster*) pour permettre une bascule immédiate des bases de données.

Deux serveurs de management pour le support clients et un serveur de management pour le support VIT ont été ajoutés.

Il n'existe pas de procédure de basculement sur l'infrastructure DR, à ce niveau tout est automatisé (*cette information est annotée dans la procédure de vérification de l'état du Failover Cluster*). Les serveurs de production Citrix DR sont accessibles à tout moment. La configuration du Failover Cluster permet dès la perte du Quorum, une bascule automatique des bases SQL active sur le site DR sans perte de données. Par contre plusieurs tâches opérationnelles ont été créées et affectées au VIT :

- Hebdomadaire : Vérification du fonctionnement du DFR-R,
- Hebdomadaire : Vérification de l'état du Failover Cluster,
- Hebdomadaire : Vérification de l'état des bases SQL et de la technologie Always on.

Cartographie Intranet (*Annexe 6*)

Le service Intranet du groupe est complété avec l'ajout d'un serveur Microsoft SQL Always On dans le site DR.

La procédure de basculement sur l'infrastructure DR se fait de façon automatique, il n'y a donc pas de procédure associée.

Plusieurs tâches opérationnelles ont été ajoutées et affectées au VIT :

- Quotidienne : Vérification de l'état du Failover Cluster,
- Quotidienne : Vérification de l'état des bases SQL et de la technologie AlwaysOn.

Cartographie EasyVista (*Annexe 6*)

L'ensemble de l'infrastructure en place a été dupliqué sur le site DR.

Pour les serveurs SQL, la technologie Microsoft AlwaysOn On a été mise en œuvre.

Le serveur applicatif ainsi que le web serveur ont été cloné via Vpshere et dupliqué, un nouveau serveur AD-LDS a été installé.

La procédure de basculement sur l'infrastructure EasyVista DR se trouve dans l'intranet département VIT.

Plusieurs tâches opérationnelles ont été ajoutées et affectées au VIT :

- Vérification de l'état du Failover Cluster,
- Vérification de l'état des bases SQL et de la technologie AlwaysOn,
- Vérification de la connectivité Active Directory (*AD-LDS*),

Le basculement vers l'infrastructure DR se fait de manière manuelle (*modification d'enregistrement DNS*) et, est liée au temps de réplication DNS. La procédure se trouve dans l'intranet, département VIT.

Cartographie Téléphonie (*Annexe 6*)

L'infrastructure téléphonique a été complétée avec l'ajout d'une Appliance Cisco Call Manager. Un cluster a été créé entre les deux nœuds, Datacenter et Datarecovery.

Le système de basculement est géré de manière automatique par le Cluster, la copie des configurations est aussi gérée de manière automatique. Il n'y a donc pas de procédure de basculement.

Il n'y a pas de nouvelle Tâche Opérationnelle liée à l'ajout de l'Appliance Cisco Call Manager.

2.2.4.3 Plan de repli et logistique

Le Plan de repli est le dispositif nécessaire à la reprise d'activité en cas de sinistre affectant les locaux habituels des utilisateurs.

Il se compose :

- Des locaux de secours, où doivent se replier les utilisateurs en cas de sinistre sur le site principal.
- Des procédures et de la documentation du secours utilisateurs : le plan de reprise global et les procédures de secours métier.
- De l'organisation de crise à déployer lors du sinistre : la liste des personnes à mobiliser en cas de sinistre, la cascade d'appels pour le déclenchement, etc.

2.2.4.4 Pour le système d'information

Il existe aujourd'hui deux types de possibilités différentes pour les entreprises qui désirent bénéficier d'une solution de repli afin d'assurer la continuité de leurs activités critiques. Soit, organiser le site de repli dans ses propres locaux, mais pour cela il faut que l'entreprise ait les possibilités financières de pouvoir le faire, soit disposer d'un site de repli chez un prestataire spécialisé, avec des solutions unique ou mutualisée.

Chacune de ces solutions présente des avantages et des inconvénients, chaque entreprise doit donc choisir la formule qui lui convient le mieux.

Il a été fait le choix d'une solution de repli interne croisé (Annexe 5), solution qui est par ailleurs la plus souvent retenue, car cela présente plusieurs avantages :

- Nous disposons des locaux et de surface suffisante,
- Les sites de Lausanne et Genève sont suffisamment distants l'un de l'autre,
- L'investissement est faible (*bureau + chaise + switch, câblage supplémentaire*),
- Les collaborateurs connaissent déjà les locaux et l'emplacement des bureaux,
- Pas de relation avec un prestataire a gérer,
- Les tests sont faciles à réaliser,
- Les modifications sont faciles à apporter dès lors qu'il y a un problème,
- Les évolutions (*effectifs/moyens*) sont rapides à mettre en œuvre,
- Maîtrise de la partie réseau et des débits.

La mise en place du site repli utilisateur se fait par la mise en œuvre des moyens dédiés, ordinateurs portables, téléphones fixes, prises Ethernet brassées, etc.… La mise en œuvre et le maintien en condition opérationnelle du site sont à la charge du VIT.

Les services concernés par le plan de repli sont uniquement les services actuellement équipés d'ordinateurs fixes, qui ne disposent donc pas de moyen de se connecter autrement que sur site : les services Ressources Humaines, Comptabilité et Administration sont donc concernés. Il est évident que

l'évaluation du nombre d'employés de chaque service devant se déplacer sur le site opérationnel est à la discrétion du responsable du service. Il a été préparé un minimum de 10 places de bureau ainsi qu'une mise à disposition de 10 ordinateurs portables par site.

Le service des Ressources Humaines doit être informé de tout déplacement de personnel sur un autre site que son lieu de travail habituel. Les frais engagés pour le déplacement du personnel donnent lieu à des remboursements de frais. A noté qu'il est préférable, dans la mesure du possible, d'utiliser les transports en commun.

Des modifications logistiques ont été apportées : Le site de Genève est celui qui a été préparé pour la plus grande absorption de personnel (*10 à 15*), les services concernés étant quantitativement plus représentés sur Lausanne. L'Open space Lanexpert ingénieur, du deuxième étage a donc été préparé. Des bureaux et nouvelles chaises ont été acquis et positionnés afin de permettre au personnel des différents services de s'installer. Il n'y a pas d'attribution de place précise, chaque personne peut s'installer ou elle le désire. Le réseau Wi-Fi de production est accessible à chaque emplacement.

Un projet spécifique intitulé « Survey Wifi » et des tests d'analyses ont été effectués à cet effet. Les prises Ethernet (*marquées avec une pastille rouge*) sont précâblées, les configurations des commutateurs sont réalisées (*Vlan production*). Le passage des ports en mode actif est à la charge du VIT.

Sur le site de Lausanne, l'Open space Lanexpert ingénieur du troisième étage a été réorganisé. L'espace du bureau a été divisé par deux par l'ajout d'armoires qui permettront d'isoler temporairement les ingénieurs consultants des autres services.

Il a aussi été mené une étude Wi-Fi pour s'assurer de la bonne diffusion du réseau de production et des prises Ethernet ont été précâblées (*marquage pastille rouge*).

Pour tous ces personnels, un ordinateur portable de prêt est déjà en fonction dans chaque service.

De plus, le VIT gère un ensemble d'ordinateurs de prêt (*sans système d'exploitation, visible/réservable dans l'intranet/VIT*) et un ensemble (*20 à 25*) d'ordinateurs préinstallés. Sur les sites de Lausanne et Genève, dix ordinateurs de prêt (*catégorie ingénieur*) sont disponibles et prêts à être installés sur les bureaux lors d'une crise. Les systèmes d'exploitation de ces ordinateurs portables sont maintenus à jour par la VIT (*mise à jour des sécurités, évolution logicielle, vérification de l'inscription au domaine, etc.*), ces ordinateurs portables profitent des mêmes garanties que les ordinateurs de production.

En ce qui concerne les imprimantes, chaque Open space dispose d'une imprimante réseau déjà configurée et en fonction.

Pour le bureau de Lausanne, il a été fait acquisition de nouvelles places de parking. Une communication du Service VIT a eu lieu à cet effet (*document ci-joint dans le PRL*).

Afin de permettre une bonne organisation du travail et une communication plus aisée, un plan des étages concernés par les zones de repli a été joint au Plan de repli et logistique.

2.2.4.5 Pour la Téléphonie

Pour la téléphonie, la solution de repli externe a été préférée. En effet, comme il n'est pas envisageable que nos clients ou nos partenaires ne puissent plus nous joindre et que notre solution téléphonique est entièrement IP, il a été développé par la société Lanexpert des scripts qui permettent de basculer automatiquement tout ou partie des lignes téléphoniques directement vers notre prestataire.

Les lignes peuvent donc être déviées soit directement via l'intranet (*exemple dessous*) soit via appel au prestataire (*Digicall*).

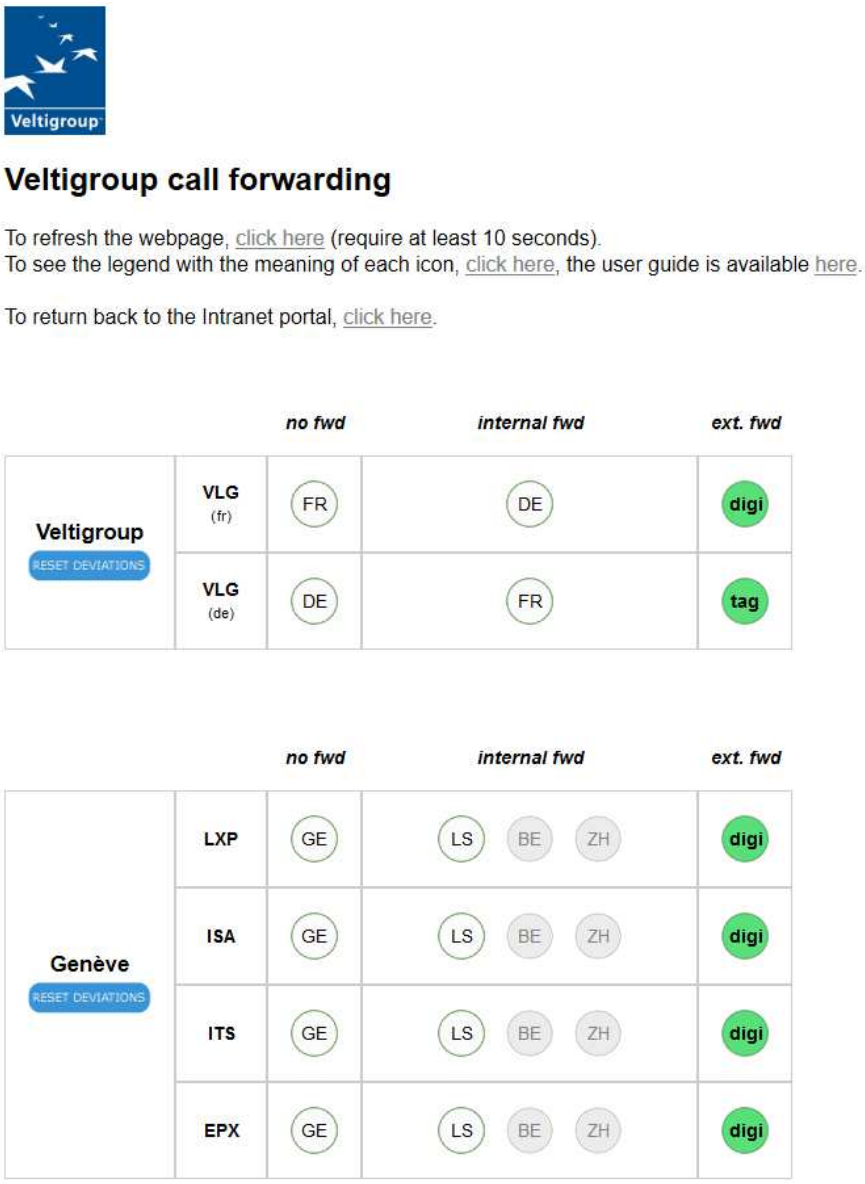


Fig. XXI : Exemple de pages web développées pour le basculement des lignes téléphoniques

2.2.5 Gestion de la crise

La gestion de la crise est réalisée par un nombre restreint de personnes organisées en cellule de crise. La cellule de crise joue le rôle d'interface entre la direction et les acteurs opérationnels, sa composition et les coordonnées de tous les membres sont inclus dans le Plan de Continuité d'Activité.

2.2.5.1 Création et définition de la cellule de crise

La cellule de crise est composée de membres permanents et de membres mobilisables qui seront appelés à participer à cette cellule si des décisions qui concernent leurs services sont à prendre. Les membres permanents sont au nombre de trois, le directeur de crise, le responsable du PCA et le responsable logistique, chacun d'eux a un rôle clé.

L'affectation de chacun de rôles listés ci-dessous a été validée lors d'un COPIL et a donné lieu à un avenant du contrat de travail et du certificat du travail, signé par chacun des partis.

Le directeur de crise : il a pour rôle d'arbitrer lorsque des décisions stratégiques doivent être prises. Il a été décidé que ce rôle reviendrait à un agent de direction déjà en charge du système de contrôle interne (*SCI*) du groupe. Ceci pour plusieurs raisons : Le statut d'agent de direction permettra d'apporter quelques réponses aux autres agents de direction lors des COPIL si nécessaire et le statut de responsable du SCI permettra un retour d'expérience pour la mise en œuvre de nouveaux contrôles forcément nécessaire.

Le responsable du PCA : son rôle est de coordonner les actions décidées lors des réunions de la cellule crise. Il doit aussi communiquer avec l'ensemble des intervenants, secours, prestataires, afin de coordonner les interventions. Il a été décidé que ce rôle reviendrait au responsable du Système d'Information (*SI*) car les responsables du SI et SCI travaillent déjà en étroite collaboration lors des contrôles internes.

Le responsable logistique : il a pour mission la mise à disposition des outils et des moyens nécessaires à la cellule de crise. Il assure l'intendance de l'entreprise et s'assure de la mise en œuvre des mesures de sécurité, évacuation, coupure d'électricité, etc. Il est en lien direct avec le responsable du PCA, les secours et les prestataires.

Les supports mobilisables par site : il y a un support technique mobilisable pour les sites de Lausanne et Genève. Ces supports mobilisables ont pour rôle d'appliquer les décisions techniques décidées par la cellule de crise. Ces supports sont sélectionnés au sein du VIT. Il nous semble primordial que ces supports aient une connaissance des infrastructures informatiques en place pour être le plus efficient possible.

Les supports mobilisables par service : tous les responsables de service sont « déclarés » mobilisables. Afin d'éviter que des informations et/ou des décisions se contredisent, il a été décidé que les responsables de service selon leur degré d'implication dans la crise en cours peuvent être mobilisés.

Tableau XIV : Tableau représentant la composition de la cellule de crise Veltigroup

Composition de la cellule de crise Veltigroup		
Mr Claude Chollet	Agent de direction	Directeur de crise
Mr Claude Chollet	Responsable SCI	Gestion des risques
Mr Claudio Simone	Responsable informatique	Responsable de la cellule de crise et du PCA
Mr Laurent Arnold	Responsable Services Généraux	Responsable logistique
Mr Thomas Tellier	Support technique (mobilisable) Site Genève	Consultant
Mr Lionel Monnier	Support technique (mobilisable) Site Lausanne	Consultant
Mme Joncour Mary-Laure	Ressources Humaines	Responsable RH
Mr Alain Stocker	Support Client (mobilisable)	Consultant
Mr Alexandre Cudre-Mauroux	Support (mobilisable)	Responsable Marketing & comm
Mr Nicolas Blanc	Support (mobilisable)	Responsable Comptabilité
Mr Sebastien Pittet	Support (mobilisable)	Responsable Bizdev et Kam
Mr Marc Antoine Busigny	Support (mobilisable)	Responsable Administration
Mr René Benard	Support (mobilisable)	Responsable Formation

Fig. XXII : Représentation cellule de crise

2.2.5.2 Réunion de la cellule de crise

Deux salles de réunion, une à Genève (*salle Jura – 2ème Étage*) et une à Lausanne (Salle K2-RDC) sont réservées pour le bon fonctionnement des réunions de la cellule de crise. Selon le site impacté et la nature de la crise, l'une ou l'autre des salles sera préférée.

L'annuaire Microsoft Exchange du groupe a été modifié pour indiquer pour chacune des deux salles, la priorité de la cellule de crise en cas ou la salle serait déjà réservée pour la tenue d'un meeting entre collaborateurs.

Toutes les décisions prises par la cellule de crise sont annotées par le responsable du PCA dans une main courante, accessible dans l'intranet (*droits limités*). Le cas échéant, si l'outil informatique est momentanément défaillant, l'ensemble de ces notes devra être réalisé par écrits.

Une fiche de qualification de l'alerte a été développée. Elle doit permettre, une fois l'alerte déclenchée, au Responsable du PCA de qualifier l'alerte et d'utiliser la « fiche réflexe » adéquate (*cf Pilotage de la crise*).

Tous les documents utilisés pour gérer la crise sont accessibles sur l'intranet pour la version dématérialisée. Une version papier est disponible à l'entrée de chacun des sites, sur demande au service Administration, dans les salles VIT à l'intérieur des coffres blindés, ignifugés.

Fig. XXIII. Extrait de la fiche de la salle de réunion « jura » de l'annuaire MS Exchange.

2.2.5.3 Documents créés pour l'alerte

Un document a été développé afin de permettre un signalement de l'alerte qui soit équivoque et sur lequel la cellule de crise puisse annoter ses décisions. Ce document appelé « Fiche de remontée d'alerte » (*annexe 1*) est accessible :

- Sur l'intranet si l'outil informatique le permet lors de l'incident,
- À l'accueil de chaque bureau, au service administration,
- Dans le coffre-fort de chaque bureau (*accessible au service Administration et VIT*).

Cette fiche permet au collaborateur qui est témoin de l'incident, de le dater, de le qualifier : incendie, inondation, etc..., de stipuler si les bâtiments sont toujours accessibles par les employés, d'informer d'éventuels blessés et donc d'une intervention en cours des services d'urgence et enfin de la présence des médias sur le site.

Il y est aussi annoté pour rappel, les numéros d'urgence des différents services, Police, Pompiers, Hôpitaux.

De plus, pour que le témoin de l'incident sache comment et à qui communiquer ces informations, un autre document intitulé « Fiche de remontée d'information » a été joint (*voir annexe 2*). Composé en deux parties, il permet selon le type d'incident rencontré de savoir comment la remontée d'information doit se faire et à qui il faut s'adresser.

Enfin, un autre document a été mis à disposition du Responsable du PCA, il s'intitule « Fiche de qualification de l'alerte » (*voir annexe 3*). Ce document a pour but de donner une base fiable à l'ouverture de la première cellule de crise. En plus des éléments de la « fiche de remontées d'alerte », l'ensemble des membres de la cellule de crise qui sont présents est annoté.

Indépendamment des documents créés pour la gestion des alertes, son déclenchement et son escalade, des annuaires ont été joints au PCA et disposé à chaque accueil des bureaux de LS et GE ainsi que dans l'intranet. Il s'agit de l'annuaire des services d'urgences : pompiers, police, hôpitaux, ainsi que l'annuaire des prestataires Veltigroup. Tous les liens vers les documents contractuels qui lient les sociétés sont spécifiés. Une grille « Prestataires de services » est aussi disponible à l'intérieur du PCA, elle récapitule pour chaque prestataire, le numéro du contrat sur lequel retrouver le niveau de support attendu, ainsi que le temps d'intervention maximum sur site.

2.2.5.4 Pilotage de la crise

Dans le cadre d'un pilotage d'une crise qui soit le plus efficient possible, un **plan de communication** a été défini. Il donne succinctement l'ordre dans lequel il est souhaitable que le groupe communique et quel service intervient dans telle ou telle phase de communication.

Les différents destinataires de la communication de groupe en temps de crise sont :

Tableau XXV : Tableau sur les phases de communication

Phase de communication	Émetteur	Destinataires	Moyens de communication	Informations essentielles
Début de crise	Témoin	Membre de la cellule de crise	Téléphone, Mail, SMS	• Circonstance de l'incident • Le lieu
Phase de crise	Cellule de crise	Collaborateurs du site	Mail, Vocal	• Circonstance et qualification de l'incident • Solution de continuité envisagée (replis, basculement, etc) • Évolution de la situation
	Cellule de crise	Collaborateurs des autres sites	Mail	• Circonstance et qualification de l'incident • Évolution de la situation
	Marketing & Communication	Clients et/ou fournisseurs	Téléphone, Mail	• Circonstance et qualification de l'incident • Mesures prises pour assurer la continuité des services
	Direction	Comité de direction	Mail/Réunion	• Circonstance et qualification de l'incident • Les mesures, les impacts immédiats
Sortie de crise	Cellule de crise	Collaborateurs du site	Mail	• Les causes de l'incident • Les conséquences • Le retour sur site si possible
	Cellule de crise	Collaborateurs des autres sites	Mail	• Les causes de l'incident • Les conséquences
	Marketing & Communication	Clients et/ou fournisseurs	Téléphone, Mail	• La fin de l'incident et retour de service • Le dédommagement
	Direction	Comité de direction	Mail/Réunion	• Les causes de l'incident • Les conséquences • Les « nouvelles »mesures de sécurité prises

Pour un pilotage de la crise rapide et efficace, un certain nombre de « fiches réflexes » (*exemple de 2 fiches réflexes en annexe 4*) ont été développées. À chacune de ces fiches réflexes correspond un type d'incident dont l'impact a été analysé dans la 1ère partie du projet. Ces fiches réflexes sont accessibles par la cellule de crise et par le responsable du PCA. Elles définissent selon le type de sinistre, les différentes étapes du début de la phase d'alerte au pilotage de la crise. La suite logique d'action à mener est définie ainsi que la liste des plans qui doivent entrer en action.

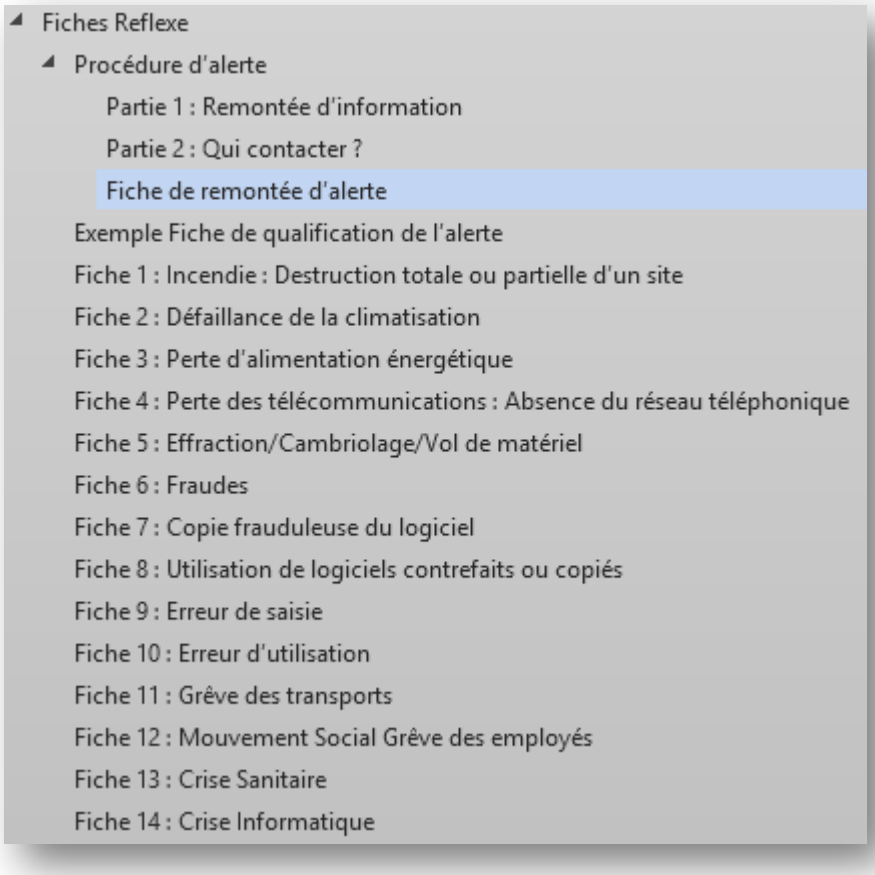


Fig. XXIV : Liste des fiches réflexes présentent dans le PCA

2.2.5.5 Sortie de la crise

La phase de sortie de crise doit permettre un retour d'expérience, elle doit permettre de tirer les enseignements de ce qui a bien fonctionné et mal fonctionné. C'est pendant la sortie de crise qu'il faut dégager les axes d'améliorations. La main courante rédigée par le Responsable du PCA doit être utilisée à cet effet. Il faudra utiliser l'ensemble des informations qui ont été notées afin d'améliorer les procédures en places.

La phase de sortie de crise doit aussi permettre un retour à un mode de fonctionnement normal du système d'information. Si le plan de secours informatique a été enclenché, il sera nécessaire, une fois la crise passée, de rebasculer les systèmes actifs dans le Datacenter.

Pour les technologies mises en œuvre ou le système de bascule se réalise de manière automatique, il faudra apporter les vérifications nécessaires pour être certain que tout fonctionne de nouveau correctement et vérifier que les services sont rétablis. Pour les autres technologies, celles qui nécessitent une intervention manuelle, toutes les procédures ont été écrites et se trouvent dans l'intranet dans la partie VIT. Ces procédures ne sont accessibles que pour le service VIT, qui est chargé de la gestion du système d'information.

Il ne faut surtout pas négliger la partie communication qui est tout aussi importante en interne comme en externe, les détails se trouvent dans le plan de communication.

2.2.6 Tests et maintien en Condition opérationnelle (*MCO*)

Le maintien en Condition opérationnelle du plan de continuité d'activité incombe au responsable du PCA et au responsable du SCI. En ce qui concerne responsable du PCA, lui est affecté un certain nombre de tâches opérationnelles qui sont qualifiées dans le temps (le plus souvent annuellement), le suivi de ces tâches opérationnelles est inscrit dans le logiciel de gestion des tickets Easyvista et dans une section de l'intranet dédiée à la maitrise des risques de manière générale.

Au responsable du SCI sont affectés au certain nombre de contrôles qui permettent de s'assurer de la mise en œuvre des procédures prévues.

L'actualisation du PCA et la réalisation de tests permettent de garantir que les moyens prévus pour assurer les secours sont toujours exploitables et efficaces. Pour être totalement efficace, le PCA doit donc être actualisé en permanence, au moins une fois par an. L'état de l'art préconise aussi que le plan de continuité d'activité soit revu en profondeur tous les trois ans.

Pour atteindre cet objectif, plusieurs tâches opérationnelles incombant au responsable du PCA et au responsable du SCI ont été créées :

- Vérifier que toutes les procédures et documentations sont à jour (*1 fois par an*),

C'est le responsable du PCA qui est le référent de la base documentaire, il est le garant que l'ensemble de la documentation est à jour et qu'elle est accessible.

- Sensibiliser les utilisateurs (*à l'embauche puis une fois par an*),

Le responsable du PCA est invité lors des journées d'embauche (*journée new joiner*) à présenter les objectifs du plan de continuité d'activité. Une communication, généralement via l'outil de messagerie est réalisée annuellement. Cette communication permet de rappeler au personnel ou trouver la documentation.

- Identifier les évolutions dans l'organisation de l'entreprise (*permanent*),

La récolte d'information permet d'identifier les évolutions dans l'organisation du groupe. Il est important que tous les responsables soient informés de l'importance de la communication dans cette étape.

- Sensibiliser les collaborateurs à communiquer les évolutions non visibles directement (*permanent*),

De la même manière que le point précédent, il faut encourager les collaborateurs à communiquer toutes les évolutions que le responsable du PCA n'aurait pas identifiées.

- Organiser des tests (*une fois par an*),

Le responsable du PCA est le coordinateur des tests et de la mise en œuvre des différents plans de secours. Le calendrier général des résultats attendu des tests est toutefois défini par le responsable du SCI en début d'année.

- Assurer les relations avec les partenaires externes (*une fois par an*).

Comme il n'y a pas de lien hiérarchique avec les partenaires externes, il faut s'assurer de la bonne communication avec les différents acteurs.

Pour que les tests soient réalisés de manière efficace ; un plan de test doit donc être défini chaque année. Ce plan de test comprend le nom des personnes qui seront amenées à participer, leur rôle dans la mise en œuvre du plan de continuité d'activité et la définition des parties du plan de secours informatique qui vont être testées.

Il est aussi très important de bien communiquer pendant les différentes phases de test. Avant et après en ce qui concerne les clients, prestataires et fournisseurs, surtout si les tests impactent de manière de manière directe ou indirecte les échanges entre nos sociétés, exemple avec la téléphonie et la bascule des lignes vers Digicall. Mais il convient également de bien communiquer en interne afin de récolter un maximum d'information qui serviront lors du bilan des tests.

3 CONCLUSION DU MÉMOIRE

La mise en œuvre d'un Plan de Continuité d'Activité constitue un projet complexe sous plusieurs aspects. Un prérequis nécessaire pour ce type de projet stratégique est une implication forte de la direction et de tous les intervenants.

Si la mise en œuvre d'un plan de continuité est un projet en tant que tel, il s'agit plus d'une démarche globale de la part de l'entreprise. S'il y a bien des dates de début et de fin comme dans un projet, le plan de continuité d'activité est quelque chose qui doit être maintenu en fonction opérationnelle et qui doit donc être mise à jour et testé régulièrement.

Pour que cela soit possible, il y a deux axes très important à développer et entretenir : la communication et la formation, qui sont nécessaires si l'on désire avoir des résultats qui soient probants lors des tests ou lorsque, malheureusement un incident se produit.

Durant toute la durée de ce projet, j'ai pu constater à quel point il était important de communiquer avec tous les acteurs du PCA. Que ce soit avec les membres de la cellule de crise ou avec l'ensemble de personnel. Il serait illusoire de croire qu'un PCA puisse fonctionner si les collaborateurs ne savent pas quelle démarche adopter en cas d'incident : à qui s'adresser, qui joue quel rôle, où se trouvent les documents importants, où se trouvent les procédures à suivre, etc.

De plus, la complexité de ce projet vient du fait qu'il se subdivise en plusieurs sous-projets :

- Élaborer le Plan de Secours Informatique (*PSI*),
- Élaborer le Plan de repli du personnel,
- Élaborer un Plan de communication,

Chacun de ces sous-projets a ses paramètres propres qu'il faut faire valider par la direction. Ainsi, le Plan de Secours Informatique répond surtout à des obligations financières, à quels moyens mettre en œuvre pour assurer la continuité de l'activité par exemple, le plan de repli du personnel a lui d'autres obligations : comment assurer la sécurité des employés sur un autre lieu de travail que celui utiliser habituellement.

La grande difficulté que j'ai pu éprouver dans ce projet concerne la partie d'analyse et d'étude fonctionnelle. Cette première étape a pour but de définir pour chaque activité les exigences de continuité, d'examiner les enjeux, d'identifier les activités essentielles et d'évaluer les conséquences d'interruption ou de dégradation de ces activités. Pour une entreprise qui n'a jamais effectué de démarche de maîtrise des risques, tout est à construite et à faire valider par la direction.

TABLE DES ILLUSTRATIONS - FIGURES

TABLE DES ILLUSTRATIONS - TABLEAUX

BIBLIOGRAPHIE

O. CAVALLARI, O. HASSID, 2011. **Réaliser le Plan de Continuité de son Entreprise**.

B. CARREZ, A. PESSOA, A. PLANCHE, 2013. **Plan de Continuité d'Activité**, Concepts et démarche pour passer du besoin à la mise en œuvre du PCA.

E. BESLUAU, 2008. Préface de D. Guinet. - **Management de la Continuité d'activité**.

---

http://www.sgdsn.gouv.fr/IMG/pdf/Guide_PCA_SGDSN_110613_normal.pdf

https://www.clusif.asso.fr/fr/production/ouvrages/pdf/PlanContinuiteActivite.pdf

http://cyberzoide.developpez.com/securite/methodes-analyse-risques/

Réaliser le Plan de Continuité d'Activité de son entreprise. Olympe Cavallari et Olivier Hassid

http://www.case-france.com/L'analysederisquepourlesdebutants.pdf

http://www.entreprises.gouv.fr/files/files/directions_services/politique-et-enjeux/entrepreneuriat/Guide-PCA-en-cas-de-crise-majeure.pdf

http://www.patricklagadec.net/fr/pdf/cellules_crise.pdf

http://moodle.insa-toulouse.fr/pluginfile.php/44681/mod_resource/content/1/QSE2014-Solucom-4.Lagestiondecrise1.0.pdf

http://www.decitre.fr/media/pdf/feuilletage/9/7/8/2/7/4/6/0/9782746079380.pdf

http://www.journaldunet.com/solutions/0506/050628_pca.shtml

http://fr.slideshare.net/ChristopheCasalegno/pra-et-pca-plans-de-reprise-et-de-continuit-dactivite

http://www.equinox-cognizant.com/wp-content/uploads/2012/12/brochure_pca.pdf

Liste des annexes

Annexe 1 : Fiche de remonte d'alerte

Si vous êtes témoin d'un incident/accident, remplissez le document suivant et transmettez-le, le plus rapidement possible au responsable du Plan de Continuité de l'Activité (*nom et coordonnée partie 2 du document remontée d'information*).

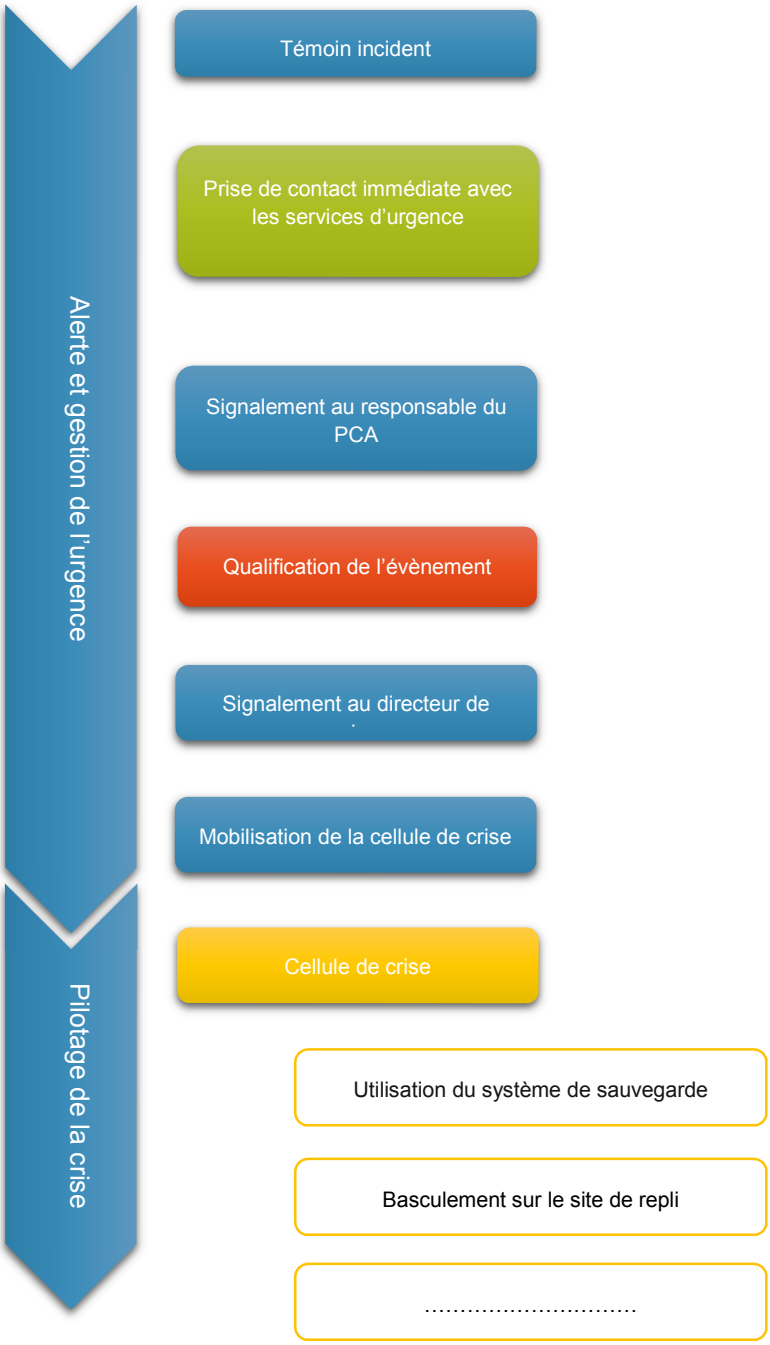
Message d'alerte	
Date de l'événement	
Heure de l'événement	
Identité du Témoin	
Nature de l'incident	❑ Incendie ❑ Défaillance climatisation ❑ Perte alimentation électrique ❑ Vol ❑ Fraudes ❑ Copie frauduleuse de logiciel ❑ Utilisation de logiciels contrefaits ❑ Perte des télécommunications ❑ Erreur de saisie ❑ Erreur d'utilisation ❑ Autres
Localisation de l'incident (Site/Service)	
Accessibilité des bâtiments	
Utilisation des infrastructures informatiques	
Victimes (si oui, nombre, nom)	
Intervention des secours	❑ Oui ❑ Non
Présence sur site des médias	❑ Oui ❑ Non

Rappel :

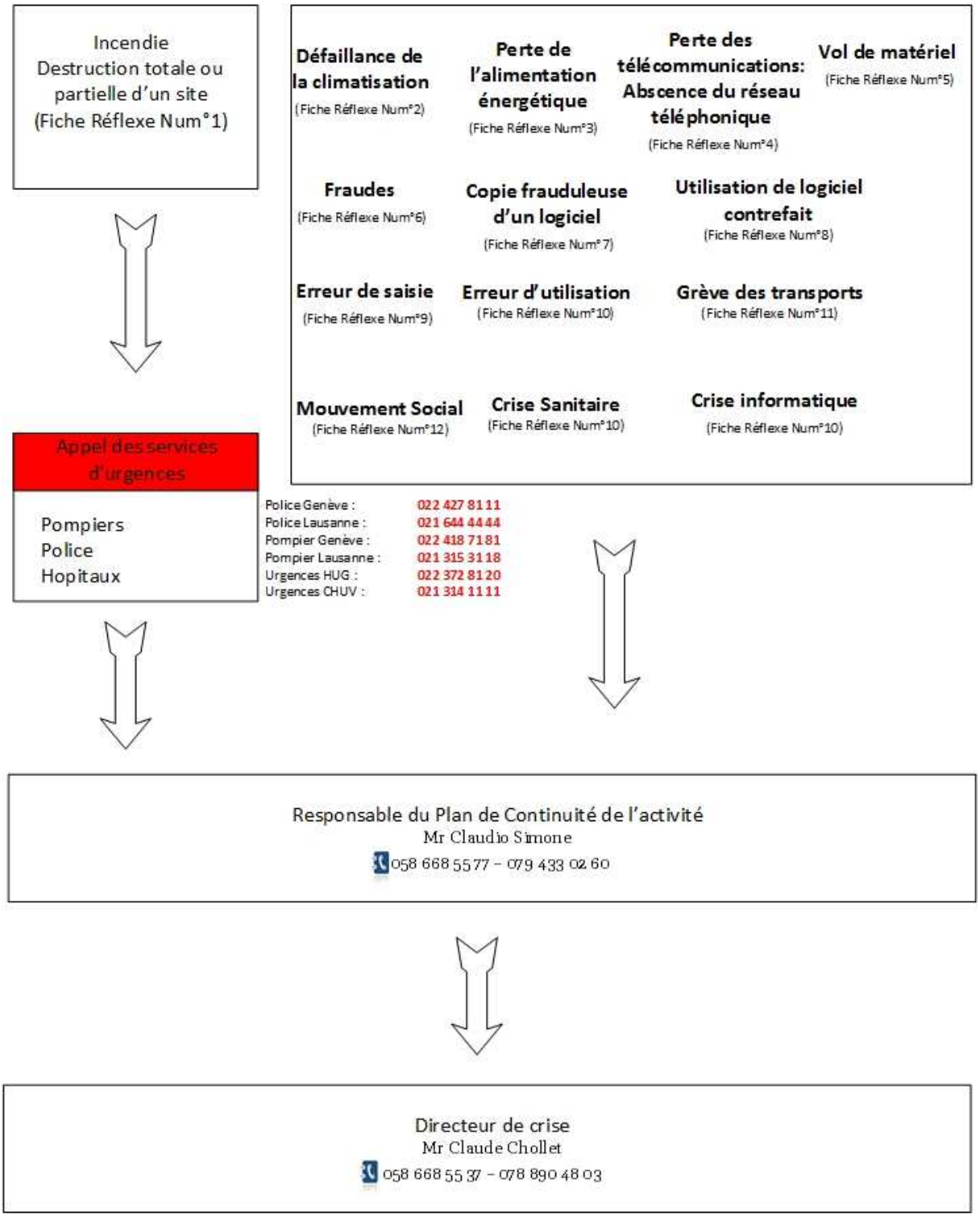
SERVICE	SITE	NUMÉRO
POLICE	Genève	022 427 81 11
POLICE	Lausanne	021 644 44 44
POMPIER	Genève	022 418 71 81
POMPIER	Lausanne	021 315 31 18
URGENCES — HUG	Genève	022 372 81 20
URGENCES – CHUV	Lausanne	021 314 11 11

Annexe 2 : Fiche de remontée d'information

PARTIE 1 : REMONTÉE D'INFORMATION



PARTIE 2 : QUI CONTACTER ?



Annexe 3 : Fiche de qualification de l'alerte

Fiche de qualification de l'alerte

Date de l'événement		
Heure de l'événement		
Identité du Témoin		
Nature de l'incident		
Localisation de l'incident		
Accessibilité des bâtiments		
Utilisation des infrastructures informatiques		
Victimes (si oui, nombre, nom)		
Intervention des secours	❑ Oui ❑ Non	
Présence sur site des médias	❑ Oui ❑ Non	
Mobilisation de la cellule de crise	❑ Oui ❑ Non	
Heure de la mobilisation de la cellule de crise		
Configuration de la cellule de crise		
Membre permanent	Directeur de crise	❑
	Responsable PCA	❑
	Responsable Logistique	❑
Support Mobilisable		
	Pour Information	Pour action
Site de Lausanne	❑	❑
Site de Genève	❑	❑
Responsable Ressources Humaines	❑	❑
Responsable Support Client	❑	❑
Responsable Marketing et Communication	❑	❑
Responsable Comptabilité	❑	❑
Responsable Bizdev et Kam	❑	❑
Responsable Administration	❑	❑
Responsable Formation	❑	❑

FICHE 1 : INCENDIE : DESTRUCTION TOTALE OU PARTIELLE D'UN SITE

Définition de la crise

- **Incendie** qui touche un site d'activité avec destruction partielle ou totale.
- **Catastrophe naturelle** qui touche un site d'activité et qui le rend indisponible (crue, tempête, tremblement de terre, inondation…).
- **Attentat** qui touche un site d'activité et qui le rend indisponible.

Plan à actionner :

- ☒ Plan de communication
- ☒ Plan de secours informatique
- ☒ Plan de relogement
- ☒ Plan de maintien des Ressources Humaines

La destruction du site liée également lié à un évènement rare ou hautement improbable fait partie de ce scénario (tremblement de terre, inondation, explosion).

Alerte et gestion de l'urgence

Pilotage de la crise

Témoin incident

Prise de contact immédiate avec les services d'urgence et les prestataires (SIG*)

Signalement au responsable du PCA

Qualification de l'évènement

Signalement au directeur de

Mobilisation de la cellule de crise

Cellule de crise

Communication

Annuaire des services d'urgence

Fiche d'alerte

- Service administratif
- Intranet
- Coffre fort

Procédure d'évacuation

- Intranet
- Plan d'évacuation mural

Annuaire des prestataires

- Annexes

***SIG : Service Industriel des villes de Genève ou Lausanne**

Composition de la cellule de crise	Actions
Membres Permanents	
Directeur de crise	• Valide l'ensemble des actions décidées lors des cellules de crise. • Valide la communication auprès des collaborateurs et la communication auprès des clients, prestataires, fournisseurs.
Responsable du PCA	• Centralise les informations auprès des services d'urgences (Hopitaux/Médecins). • Coordonne les actions décidées en cellule de crise.
Responsable Logistique	• Mise en relation avec les SIG o Coupure électrique des étages o Nettoyage/évacuation
Supports Mobilisables	
Responsable Ressources Humaines	• Lister les personnes manquantes/blessées/évacuées. • Organisation du télétravail des collaborateurs. • Mise en relation avec les assurances.
Marketing et Communication	• Assurer une communication interne, tenir informés les collaborateurs de l'évolution de la situation. • Assurer une communication externe afin de tenir informés les clients, prestataires, fournisseurs.
Service informatique	• Organisation du télétravail et mise en place du matériel de prêt.

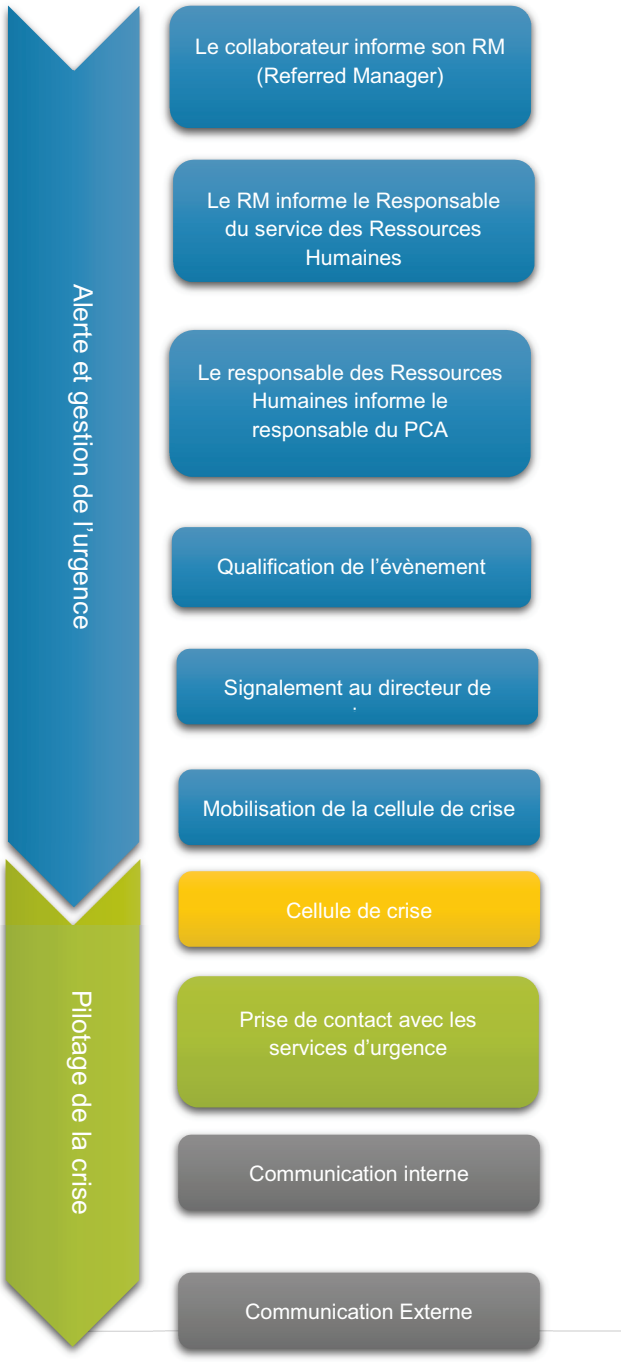
FICHE 13 : CRISE SANITAIRE

Définition de la crise

- **Crise Sanitaire** qui entraîne un fort taux d'absentéisme.

Plan à actionner :

- ☒ Plan de communication
- ❑ Plan de secours informatique
- ❑ Plan de relogement
- ☒ Plan de maintien des Ressources



Fiche d'alerte

- Service administratif
- Intranet
- Coffre fort

Annuaire des services d'urgence

- Annexes

Composition de la cellule de crise	Actions
Membres Permanents	
Directeur de crise	• Valide l'ensemble des actions décidées lors des cellules de crise.
Responsable du PCA	• Coordonne les actions décidées en cellule de crise. • Suivi et mise en place des décisions ministérielles
Responsable Logistique	• Assurer la logistique et matériel nécessaire pour la mise en œuvre des dispositions décidées en cellule de crise. • Mettre en place les mesures de nettoyage spécifiques. • Contacter les autorités afin de connaître les mesures qu'il faut appliquer au sein de la société.
Supports Mobilisables	
Responsable Ressources Humaines	• Recenser les collaborateurs qui sont absents. • Organisation du télétravail et mise en place du matériel de prêt.
Marketing et Communication	• Assurer une communication interne régulière auprès des collaborateurs afin de bien informer sur les décisions prises en cellule de crise et sur les modifications sur les organisations du travail.
Service informatique	• Organisation du télétravail et mise en place du matériel de prêt.
Responsable Comptabilité	• Évaluation du préjudice

Annexe 5 : Plan de repli et logistique

Implementation DRP
(Disaster Recovery Plan Project)

Dear colleagues,

we are pleased to announce you that as part of the project: Disaster Recovery Plan, Lausanne office and Geneva office have been fix out. In each office, a fallback zone was fitted and must allow the continuity of work in the case of a major incident will impact one or the other site.

You can retrieve all the procedure for booking laptop, phone connecting into the intranet. You can also retrieve a new menu – **Borrow Laptop** - into your MY HR menu.

Service Desk Forms

Borrow Laptop

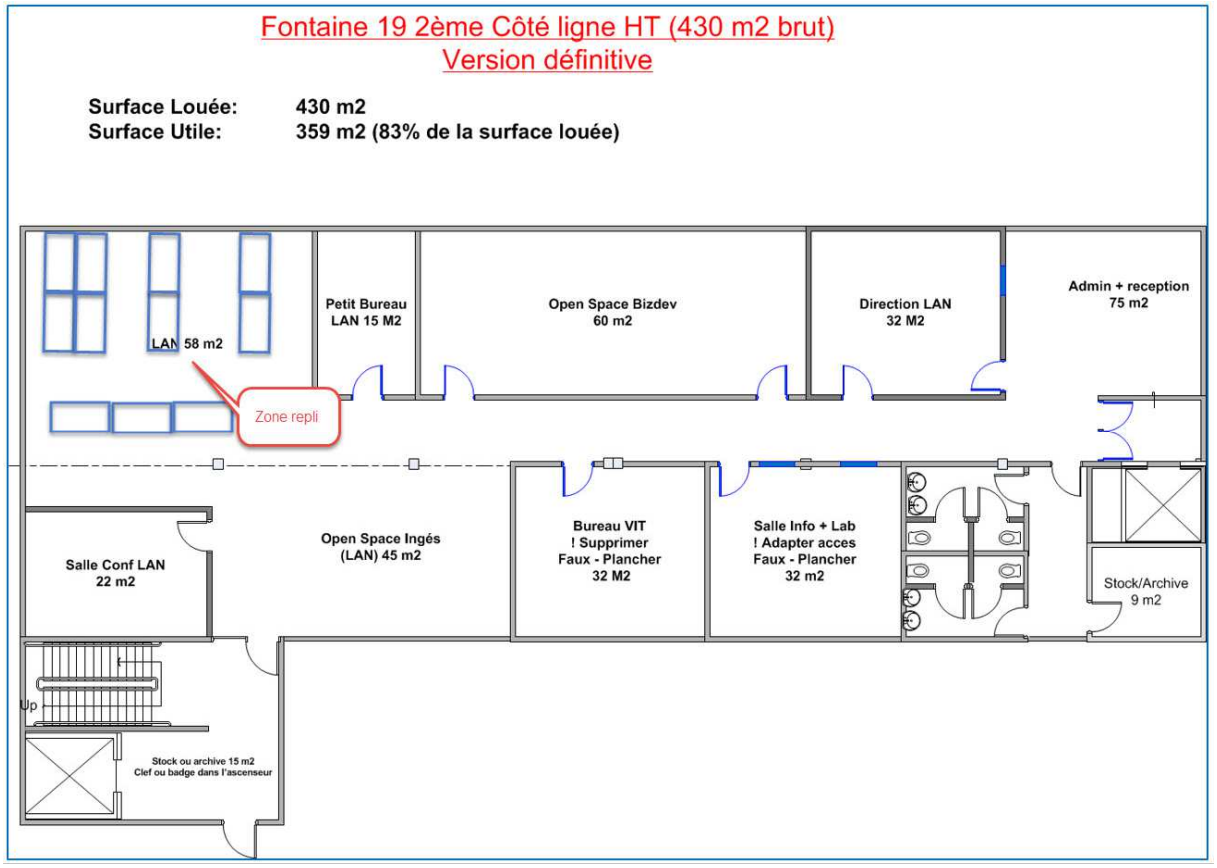
Access Rights Request

For New Laptop Order please contact the Service Desk

Be aware that possibility to move on to one or the other site can only be given by your manager !

Extrait du mail de communication envoyé aux services Back Office

Genève deuxième étage



L'emplacement appelé « zone de repli » a été aménagé afin d'accueillir le personnel de Lausanne.

Bureau

Le placement est « libre ».

Téléphone

Vous avez deux possibilités pour l'utilisation de Téléphones :

- L'utilisation des téléphones Mobiles – disponible à l'entrée de l'open space.
- La connexion à un téléphone fixe – un téléphone pour deux bureaux.

La procédure de connexion aux téléphones fixes ou mobiles est accessible dans l'intranet, menu VIT – Service –Telephonie : VIT - How work internal telephony.

Laptop

La réservation des laptop se fait dans l'intranet dans la partie personnelle, My HR(procédure disponible dans l'intranet).

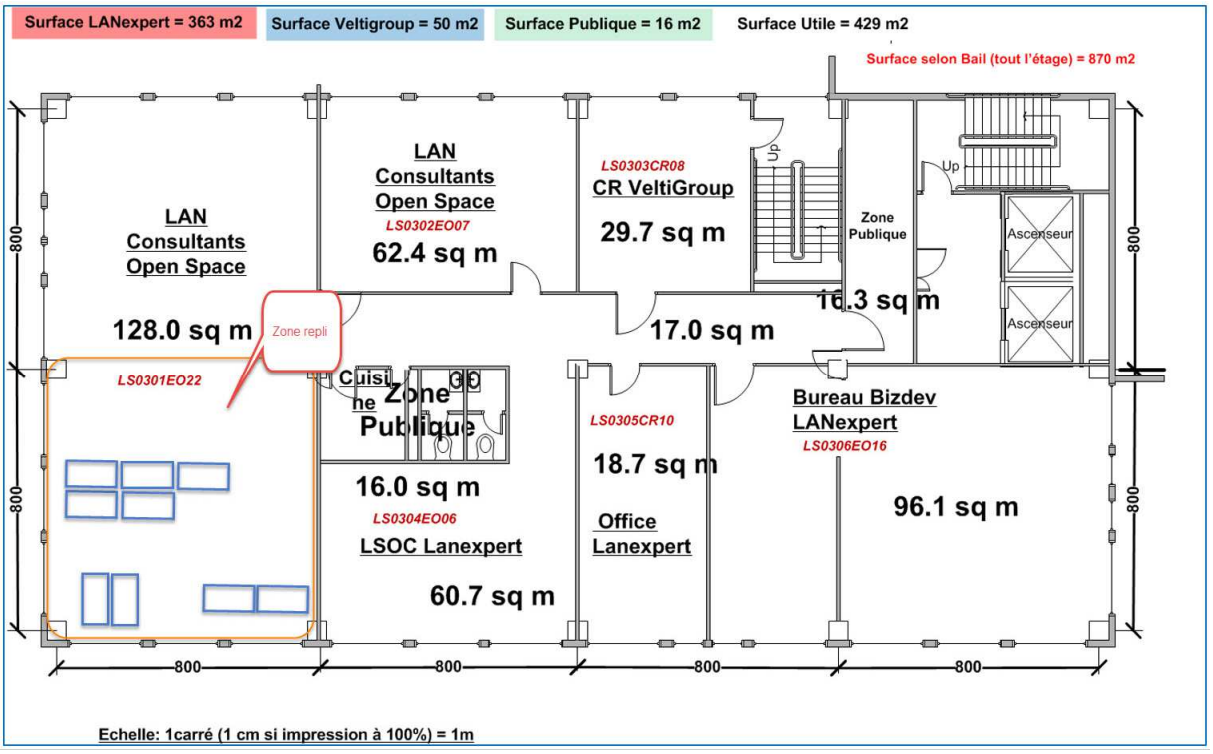
La connexion des laptop au réseau de production Wifi est déjà configurée. Pour une connexion câblée obligatoire, veuillez contacter le servicedesk.

Environnement de travail – Citrix

Pour la connexion à votre environnement de travail, l'infrastructure Citrix doit permettre une reconnexion automatique aux sessions ouvertes avant la coupure/arrêt des systèmes sur votre site normal de production.

Pour tout problème de reconnexion à vos sessions actives veuillez contacter le servicedesk.

Lausanne troisième étage



L'emplacement appelé « zone de repli » a été aménagé afin d'accueillir le personnel de Genève.

Bureau

Le placement est « libre ».

Téléphone

Vous avez deux possibilités pour l'utilisation de Téléphones :

- L'utilisation des téléphones Mobiles – disponible à l'entrée de l'open space.
- La connexion à un téléphone fixe – un téléphone pour deux bureaux.

La procédure de connexion aux téléphones fixes ou mobiles est accessible dans l'intranet, menu VIT – Service –Telephonie : VIT - How work internal telephony.

Laptop

La réservation des laptop se fait dans l'intranet dans la partie personnelle, My HR(procédure disponible dans l'intranet).

La connexion des laptop au réseau de production Wifi est déjà configurée. Pour une connexion câblée obligatoire, veuillez contacter le servicedesk.

Environnement de travail – Citrix

Pour la connexion à votre environnement de travail, l'infrastructure Citrix doit permettre une reconnexion automatique aux sessions ouvertes avant la coupure/arrêt des systèmes sur votre site normal de production.

Pour tout problème de reconnexion à vos sessions actives veuillez contacter le servicedesk.

Lausanne new parking places

News Service Desk Veltigroup

☐ Required manipulation
☐ Important information
☒ **Announcement**

People who are concerned : Recipient of this e-mail

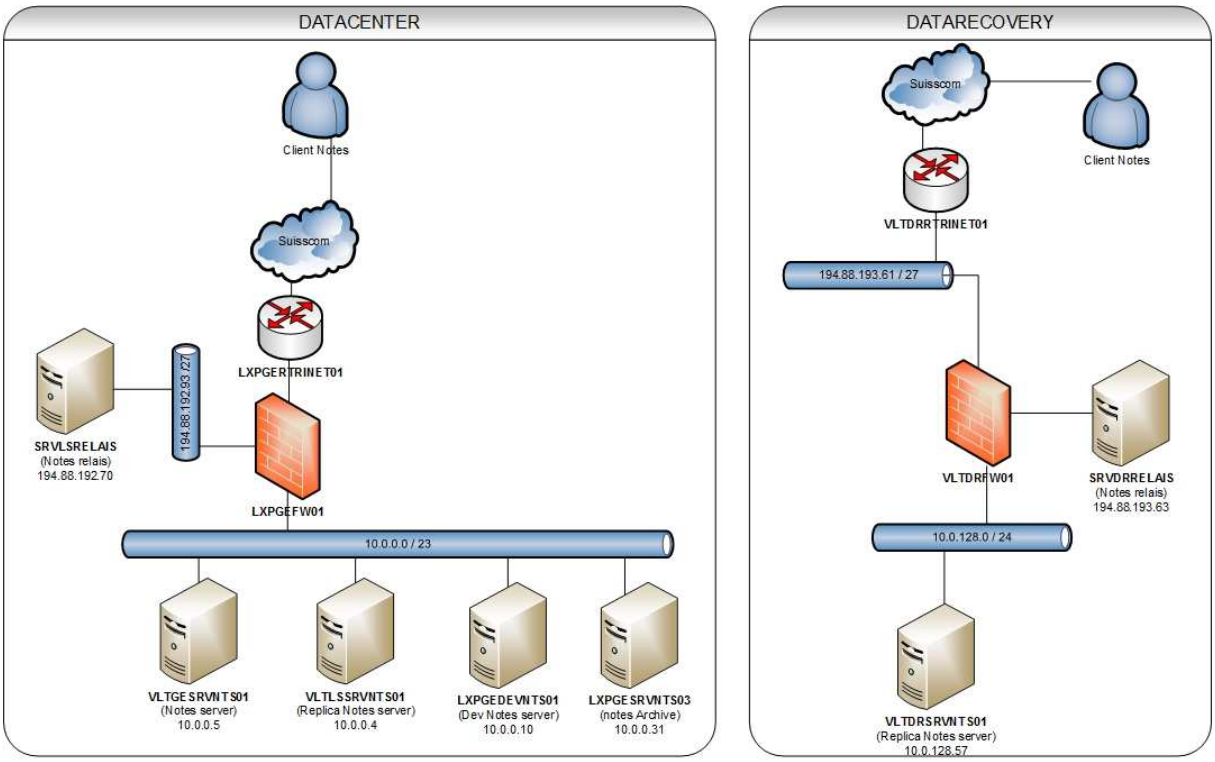
Lausanne parking places

Veltigroup acquired new places

If you have any further questions or concerns, please feel free to contact VIT ServiceDesk @ 8666.
Thank you for your cooperation,
Your VIT team

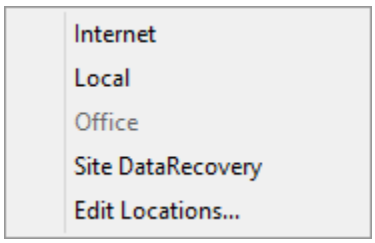
VIT Team - Veltigroup IT – contact : servicedesk@veltigroup.com - +41 22 719 86 66

Cartographie Lotus Notes

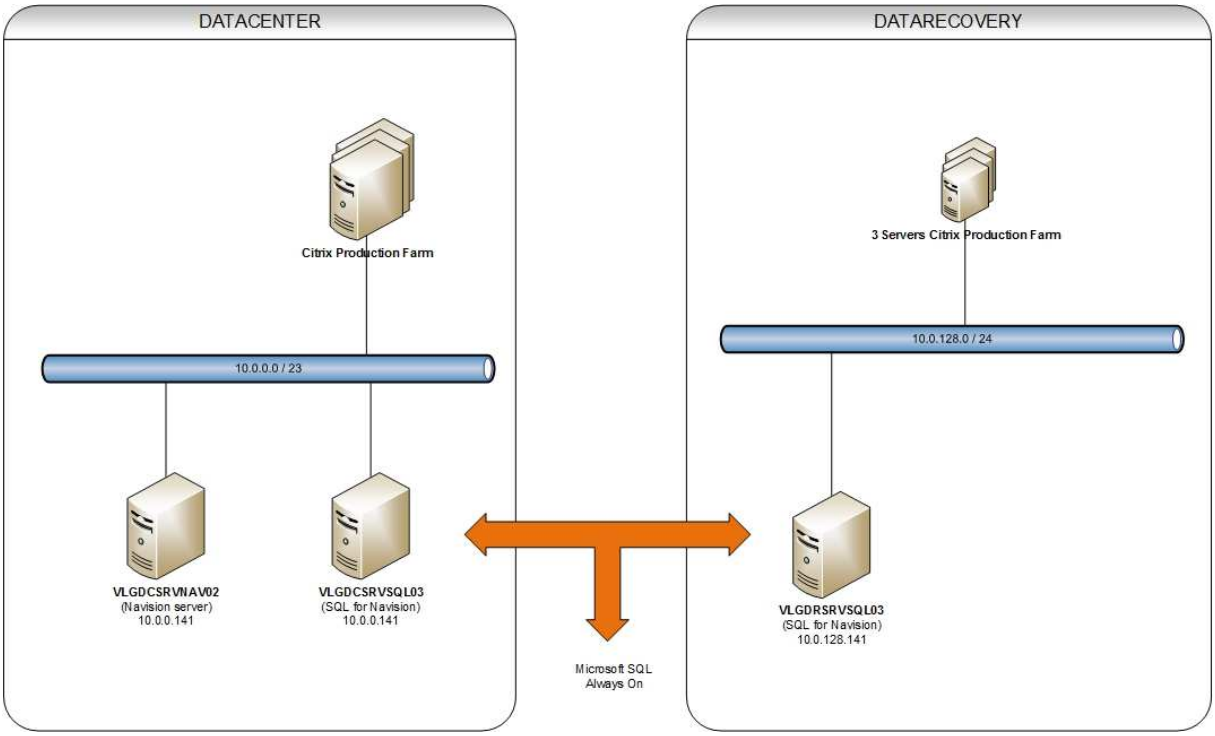


L'infrastructure Lotus Notes a été complétée avec l'ajout d'un serveur relais en DMZ DR et d'un serveur de production VLTDRSRVNTS01.

Il n'y a pas de procédure de basculement sur l'infrastructure de DR. L'utilisation de l'infrastructure Lotus Notes DR se fait par la configuration du client Notes.



La procédure pour configurer le client lotus notes se trouve dans l'intranet, département Vit (Lien : http://intranet/vit/kb/SetupGuide/Forms/AllItems.aspx?RootFolder=vitSetupGuideVITDServicesApplications \Configuration_LN. docx)



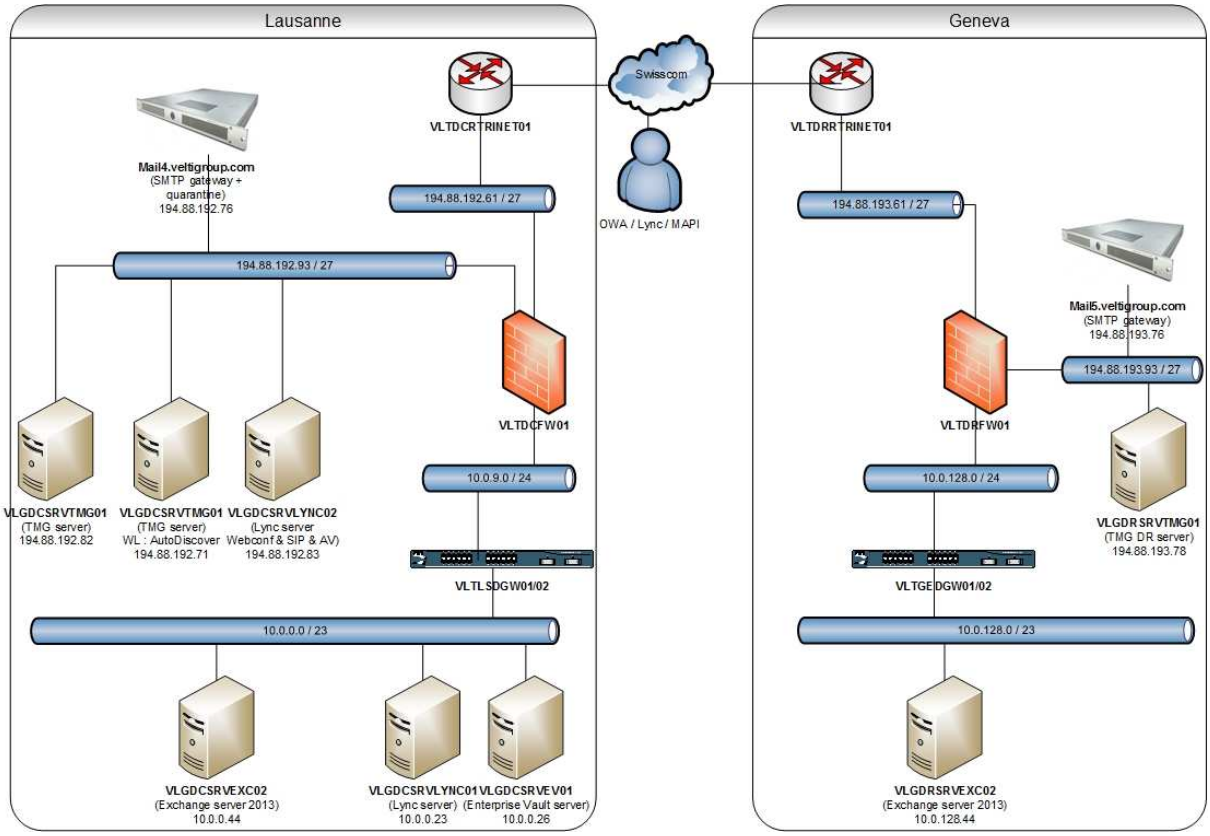
L'infrastructure de l'ERP Microsoft Dynamics Navision a été complétée dans le site DR avec l'ajout de 3 serveurs Citrix de production ainsi qu'un serveur Microsoft SQL et de la technologie AlwaysOn.

La procédure de basculement sur l'infrastructure DR se fait de façon automatique, il n'y a donc pas de procédure associée.

Plusieurs tâches opérationnelles ont été ajoutées et affectées au VIT :

- Vérification de l'état du Failover Cluster
- Vérification de l'état des bases SQL et de la technologie AlwaysOn

Cartographie Messagerie et Remote access (TMG)



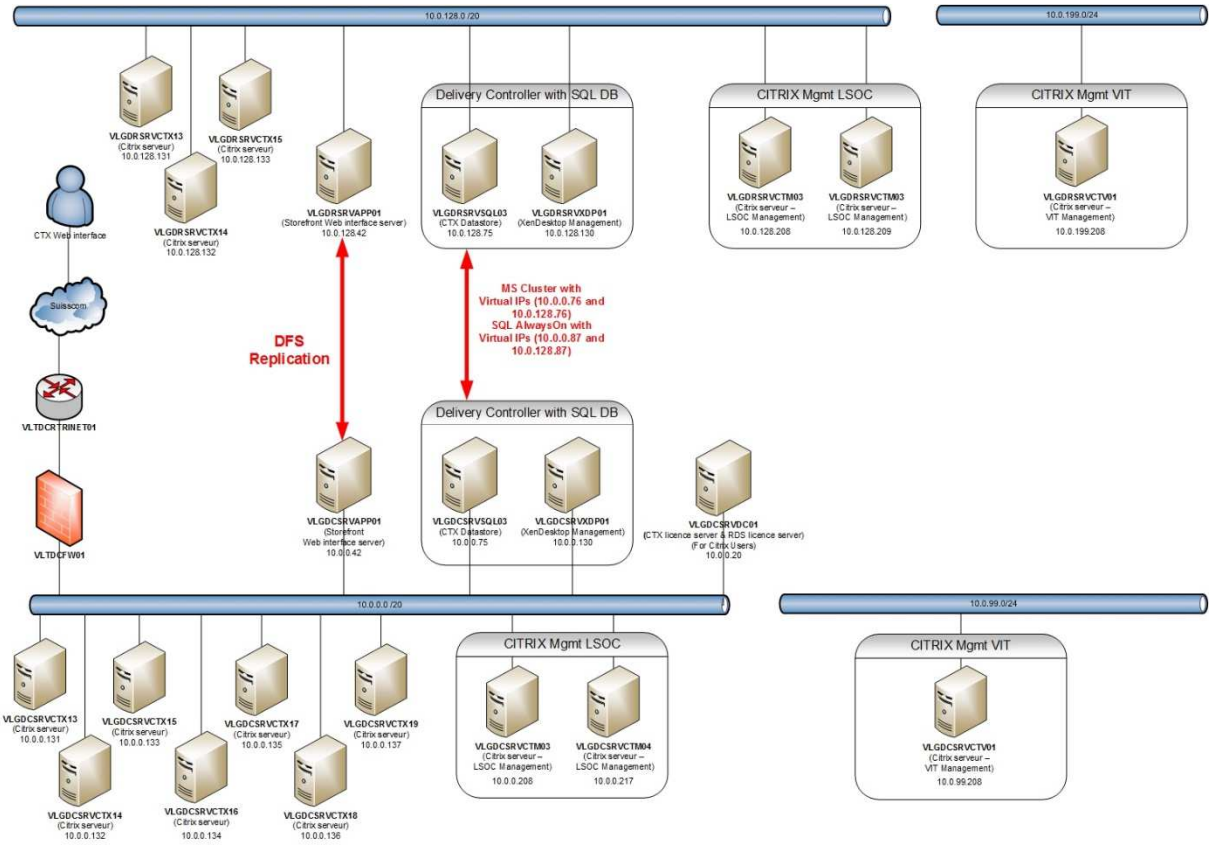
L'infrastructure de messagerie et de remote access a été modifiée de deux manières :

Une partie avec un basculement automatique avec l'ajout d'une appliance Cisco Ironport et la création d'un cluster.

Une partie avec un basculement manuel avec l'ajout d'un serveur Microsoft TMG.

La procédure de basculement manuel se trouve sur l'intranet, département VIT (Lien : http://intranet/vit/kb/SetupGuide/Forms/AllItems.aspx?RootFolder=vitSetupGuideFVITDServicesMessagerieetcommunication/TMGFailover.docx)

Nouvelle Cartographie Citrix



L'ensemble de l'infrastructure Citrix existante est dupliqué sur le site DR (10.0.128.0/20). Trois serveurs de production VLGDRSRVCTX13/14/15 sont installés. Le système d'exploitation est maintenu à jour lors des journées patching par le VIT. Le serveur Storefront (nouveau web interface) est dupliqué sur le site DR également, il contient l'ensemble des profils utilisateurs Windows qui sont dupliqués via la technologie DFS-R de Microsoft.
Un serveur SQL est configuré avec la technologie Micorosoft SQL AlwaysOn (Failover Cluster) pour permettre une bascule immédiate des bases de données.

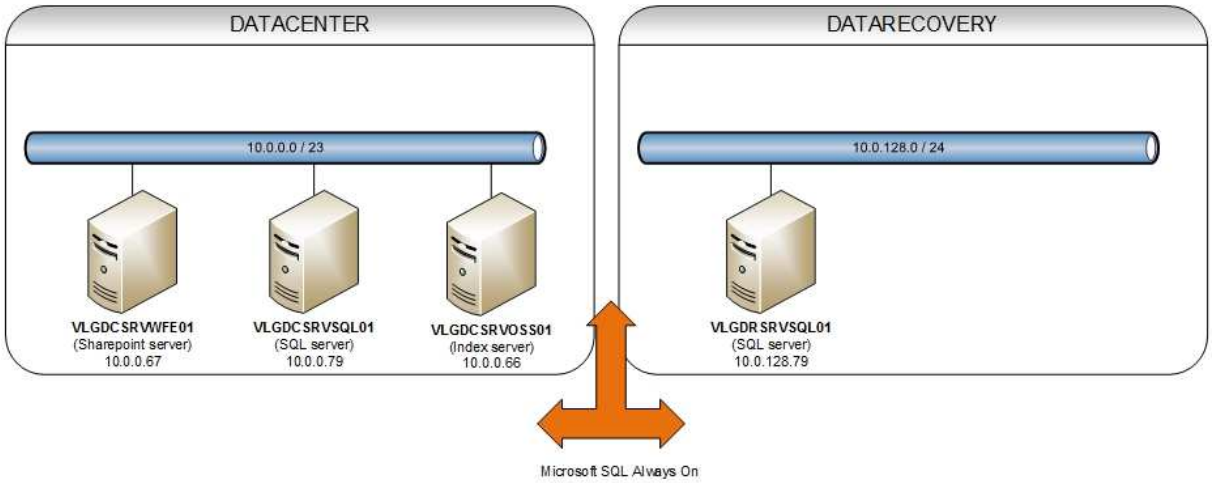
Deux serveurs de management pour le support clients et un serveur de management pour le support VIT ont été ajoutés.

Il n'y a pas de procédure de basculement sur l'infrastructure DR, à ce niveau tout est automatisé. Les serveurs de production Citrix DR sont accessibles à tout moment. La configuration du Failover Cluster permet dès la perte du Quorum une bascule automatique des bases SQL active sur le site DR sans perte de données.
Plusieurs tâches opérationnelles ont été créées et affectées au VIT :

- Vérification du fonctionnement du DFR-R
- Vérification de l'état du Failover Cluster
- Vérification de l'état des bases SQL et de la technologie AlwaysOn

Toutes les procédures se trouvent sur l'intranet, département VIT (http://intranet/vit/kb/SetupGuide/VITOperationnalTasks/VITOperationnalTasks.docx)

Cartographie Intranet



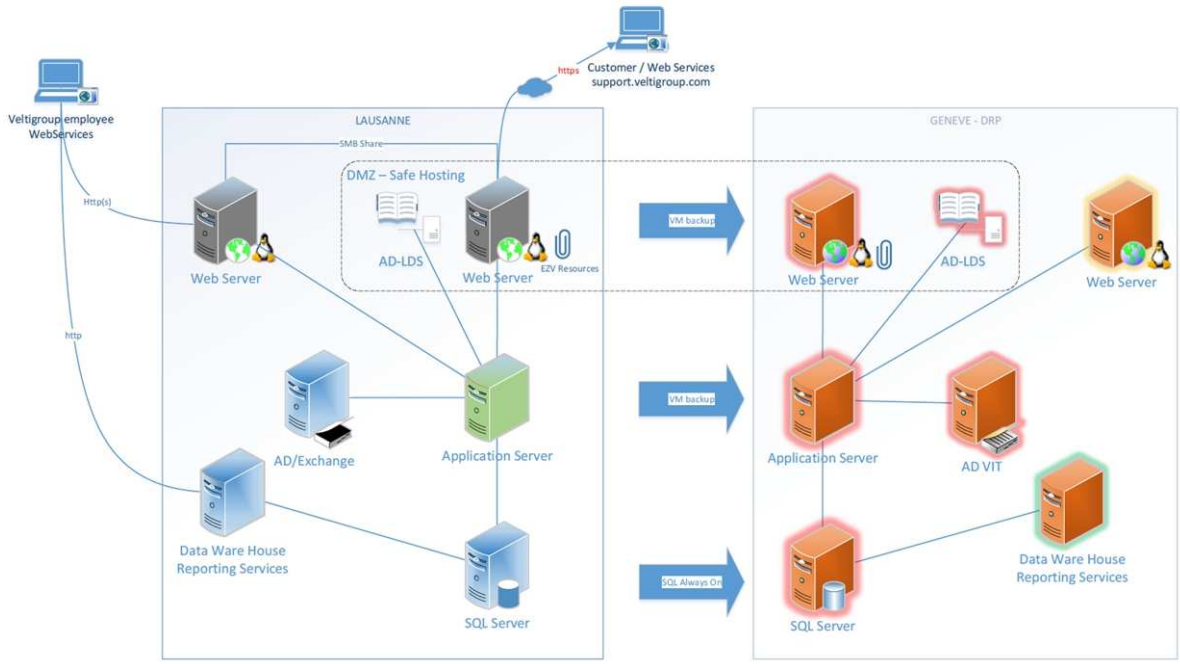
Le service Intranet du groupe est complété avec l'ajout d'un serveur Microsoft SQL AlwaysOn dans le site DR.

La procédure de basculement sur l'infrastructure DR se fait de façon automatique, il n'y a donc pas de procédure associée.

Plusieurs tâches opérationnelles ont été ajoutées et affectées au VIT :

- Vérification de l'état du Failover Cluster
- Vérification de l'état des bases SQL et de la technologie AlwaysOn

Cartographie EasyVista



L'ensemble de l'infrastructure en place a été dupliqué sur le site DR.

Pour les serveurs SQL la technologie Microsoft AlwaysOn a été mise en œuvre.

Le serveur applicatif ainsi que le web serveur ont été cloné via Vpshere et dupliqué, un nouveau serveur AD-LDS a été installé.

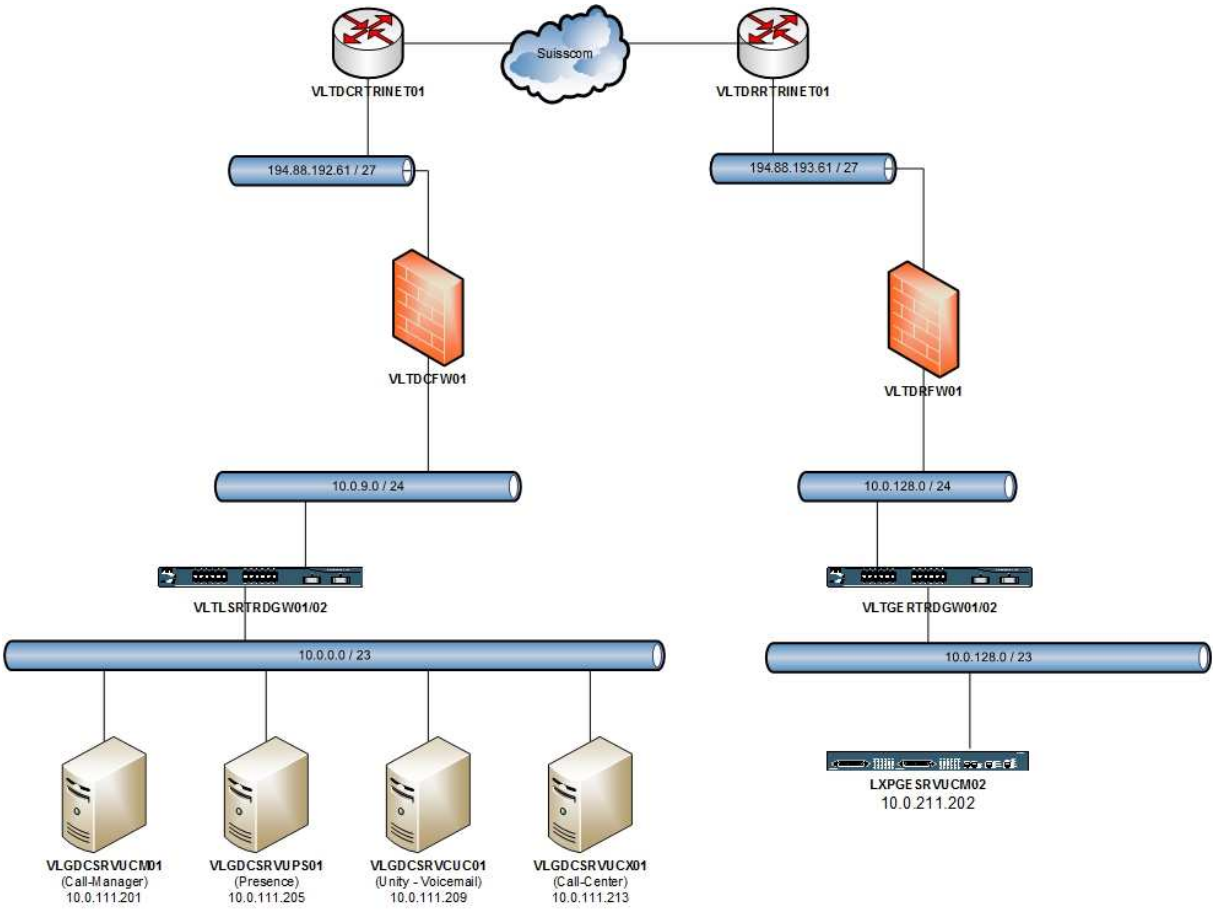
La procédure de basculement sur l'infrastructure EasyVista DR se trouve dans l'intranet département VIT (Lien :

Plusieurs tâches opérationnelles ont été ajoutées et affectées au VIT :

- Vérification de l'état du Failover Cluster
- Vérification de l'état des bases SQL et de la technologie AlwaysOn
- Vérification de la connectivité Active Directory (AD-LDS)

Le basculement vers l'infrastructure DR se fait de manière manuelle (modification d'enregistrement DNS) et est soucis au temps de réplication DNS. La procédure se trouve dans l'intranet, département VIT (Lien : http://intranet/vit/kb/SetupGuide/Forms/AllItems.aspx?RootFolder=vitSetupGuideVITDServicesApplications \Easyvista_Dr. docx)

Cartographie Téléphonie



L'infrastructure téléphonique a été complétée avec l'ajout d'une Appliance Cisco Call Manager. Un cluster a été créé entre les deux nœuds, DC et DR.

Le système de basculement est géré de manière automatique par le Cluster, la copie des configurations est aussi gérée de manière automatique. Il n'y a donc pas de procédure de basculement.

Il n'y a pas de nouvelle Tâche Opérationnelle liée à l'ajout de l'Appliance Cisco Call Manager.

Annexe 7 : Annuaire des prestataires

NOM DU PRESTATAIRE	TYPE DE PRESTATION	DESCRIPTION	CONTRAT	SITES	SUPPORT LEVEL	INTER. MAX
SWISSCOM	Ligne SES	Ligne inter-sites	PRO-004031282	GE/LS	Lundi au dimanche 24h/24 y compris jours fériés	8h
SWISSCOM	Ligne IP+	Ligne internet	PRO-004031282	GE/LS	Lundi au dimanche 24h/24 y compris jours fériés	8h
SIEMENS	Sécurité intrusion	Système anti intrusion	8280053777	GE/LS		24h
PROTECTAS	Sécurité bâtiment		002453	GE	Lundi au dimanche 08h00-18h00	
PROTECTAS	Sécurité bâtiment		002421	LS	Lundi au dimanche 24h/24 y compris jours fériés	1h
MGE SCHNEIDER UPS	Onduleur	Onduleur électrique	2003024	GE	Lundi au dimanche 24h/24	8h
MGE SCHNEIDER UPS	Onduleur	Onduleur électrique	2003021	LS	Lundi au dimanche 24h/24	8h
ULTRAFROID SA	Climatisation	Climatisation Datacenter	SEFA 2011-126.000	LS	Lundi au dimanche 24h/24	
CPA FROID SA	Climatisation	Climatisation DRP	M117/13	GE	-	-
SIG	Electricité/Eau		1177026	GE	Lundi au dimanche 24h/24	
GEDEFI	Bâtiment			GE		
BRS	Bâtiment			LS		
CISCO	Infrastructure	LAN		GE/LS	Lundi au vendredi	1J
CISCO	Infrastructure	Virtualisation		GE/LS	Lundi au vendredi	1J
CISCO	Ironport	Gateway		GE/LS	Lundi au vendredi	1J

Résumé

Concevoir un Plan de Continuité d'Activité (*PCA*) pour les applications critiques et/ou un Plan de Reprise d'Activité (*PRA*) structuré permettant de répondre à un maximum de scénarios d'incidents.

Mémoire ingénieur C.N.A.M. ; Rhône-Alpes 2016

Le groupe suisse de services informatiques Veltigroup SA est leader sur le marché de l'IT en Suisse romande et alémanique. Dans le cadre de son développement et de sa croissance le projet de mettre en œuvre un Plan de Continuité d'Activité m'a été confié durant l'année 2015/2016. Le Plan de continuité d'Activité est devenu un outil indispensable pour toutes entreprises qui veut assurer sa survie en cas de sinistre mineur ou majeur, mais offre aussi des garanties aux clients.

La réussite de ce projet est le résultat d'une action collective impliquant tous acteurs de l'entreprise et du système d'information en particulier, ingénieurs, utilisateurs et managers.

La réalisation du PCA aura permis la réalisation d'un nombre important de procédures sur les systèmes en place, mais aussi la mise en œuvre d'une multitude de sous-projets techniques. L'ensemble de ces projets a pu être confié aux ingénieurs du service VIT.

Au-delà des différents plans et moyens à mettre en œuvre en cas d'incident, il est nécessaire de réaliser des tests régulièrement afin de valider le fonctionnement des moyens de secours et ainsi faire vivre le PCA en l'améliorant constamment.

Mots clés : Projet, Plan de Continuité d'Activité, outil, système d'information, sinistre, mineur, majeur, incident, tests.

Summary

The Swiss group Veltigroup SA IT Services is a leader in the IT market in French-speaking Switzerland and German-speaking. As part of its development and growth, the project to implement a Business Continuity Plan was entrusted to me during the year 2015/2016. The Activity Continuity Plan has become an indispensable tool for all companies that want to ensure survival in the event of minor or major disaster but also provides guarantees to customers.

The success of this project is the result of collective action involving all stakeholders of the company and the information system in particular, engineers, users and managers.

The implementation of the PCA will permit the achievement of a significant number of procedures on the systems in place but also the implementation of a multitude of technical sub-projects. All these projects have been entrusted to engineers VIT service.

Beyond the different plans and means to implement it is necessary to conduct tests regularly to validate the operation of emergency equipment and thus to live the PCA by improving constantly.

Key words : Project, Business Continuity Plan, tool, information system, sinister, minor, major, incident, tests.