Le passage d'un système d'information physique à une solution virtuelle

Nicolas Damonneville

CONSERVATOIRE NATIONAL DES ARTS ET METIERS
PARIS

Mémoire présenté en vue d'obtenir
le « Diplôme d'ingénieur CNAM »
Spécialité : INFORMATIQUE

Option : Informatique réseaux, systèmes et multimédia
Code : CYC9104A

Par
DAMONNEVILLE Nicolas

Le passage d'un système d'information physique à une solution virtuelle

Soutenu le : 03/02/2022

JURY
PRESIDENT :
MEMBRES :

Remerciements

Le sujet de mon mémoire étant un projet que j'ai eu l'honneur d'effectuer au sein de la compagnie pétrolière Total, mes premiers remerciements sont tout naturellement portés à leur égard.

Cette période de travail en tant que salarié au sein de Total, plus précisément à la plateforme pétrolière de Grandpuits-Gargenville, m'a permis d'entrer progressivement dans la vie active, un souhait réel de ma part depuis l'obtention de mon Brevet de Technicien Supérieur (BTS) et de ma Licence Sciences Technologies Santé mention Informatique (STS).

Je remercie en conséquence toute l'équipe pédagogique du Conservatoire National des Arts et Métiers (CNAM) de m'avoir accordé leur confiance ainsi que de m'avoir intégré au sein du parcours « Diplôme d'Ingénieur Informatique Réseaux, Systèmes et Multimédia (IRSM) » par suite de l'obtention de mon titre de « Concepteur en Architecte Informatique, option Cybersécurité ».

Je remercie également tout le personnel de la plateforme de Grandpuits-Gargenville pour leur accueil et leur accompagnement au sein de TotalEnergies tout au long de ces années de travail. Mes pensées vont tout d'abord à Stéphane Lefebure pour toute l'aide et les conseils qu'il m'a apportés au cours des missions, travaux réalisés et aussi dans la réflexion de mon projet professionnel.

Enfin, merci à Frédéric Delgrange mon tuteur et chef du service systèmes, pour le soutien qu'il m'a apporté, tant sur le plan relationnel qu'extra-professionnel lors de mes années au sein de l'entreprise.

La compagnie TotalEnergies ayant été la première entreprise dans laquelle j'ai pu travailler lors de mon entrée dans le monde du travail, il est l'un des acteurs majeurs à la progression de ma carrière professionnelle.

Abréviations

→ **ANSSI :** Agence Nationale de la Sécurité des Systèmes d'Information

→ **BDD :** Base De Données

→ **BTS :** Brevet de Technicien Supérieur

→ **CNAM :** Conservatoire National des Arts et Métiers

→ **CPU :** Central Processing Unit

→ **DMZ :** Demilitarized Zone

→ **GO :** GigaOctet

→ **IP:** Internet Protocol

→ **IRSM :** Informatique, Réseaux, Systèmes et Multimédia

→ **PCA :** Plan de Continuité d'Activité

→ **PDG :** Président Directeur Général

→ **PLIF :** PipeLine d'Ile-de-France

→ **PRA :** Plan de Reprise d'Activité

→ **RAID :** Redundant Arrays of Inexpensive Disks

→ **RAM :** Random Access Memory

→ **SE :** Société Européenne

→ **SFP:** Small Form-factor Pluggable

→ **SGBD :** Système de Gestion de Bases de Données

→ **SIE :** Système d'Information d'Entreprise

→ **SII :** Système d'Information Industriel

→ **SNMP :** Simple Network Management Protocol

→ **SQL:** Structured Query Language

→ **STS :** Sciences Technologies Santé

→ **SVM /CVM:** Service VM / Controller VM

→ **TO :** TeraOctet

→ **UE :** Unité d'Enseignement

→ **VLAN:** Virtual Local Area Network

→ **VM :** Virtual Machine

→ **VM:** Virtual Machine

→ **VPN :** Virtual Private Network

Glossaire technique

→ **Adresse IP :** Il s'agit de l'adresse définissant un équipement informatique sur le réseau

→ **AS :** Signifie « Autonomous System », il s'agit d'une collection de protocoles internet étant sous la responsabilité d'un fournisseur d'accès internet.

→ **Asynchrone :** Il s'agit d'une technologie désynchronisée, c'est-à-dire que des informations répétées ne sont pas cohérentes à chaque instant.

→ **Base de données :** Permet le stockage de données, il s'agit d'un équipement très sensible à ne pas négliger.

→ **Cluster :** Un groupe d'équipements travaillant ensemble

→ **Cœur de réseau :** Niveau d'équipements informatique par lequel passe une majorité du trafic.

→ **Commutateur / Switch:** Équipement permettant la connexion entre les équipements d'un même réseau.

→ **CPU :** Il s'agit du processeur de l'ordinateur ou du serveur, le cœur de ce dernier.

→ **DMZ :** Il s'agit d'une zone de passage obligatoire pour un flux d'informations avant de pouvoir entrer dans le réseau.

→ **Fibre optique :** Méthode de connexion physique entre les équipements, il s'agit de la technologie avec le transfert le plus rapide.

→ **Hyperviseur / Hypervisor :** Couche logicielle permettant la gestion de machines virtuelles.

→ **Maître-Esclave :** Architecture informatique disposant de donneurs d'ordres et d'exécutants.

→ **Modèle OSI :** Modèle réseau basique définissant les 7 couches de communication entre deux équipements.

→ **Oracle :** Il s'agit de l'entreprise commercialisant le SGBD Oracle, un des produits phares dans le monde de la base de données.

→ **Paquet IP :** Format des flux de données transitant sur le réseau.

→ **Pare-feu / Firewall :** Un équipement informatique qui protège le réseau en filtrant les données.

→ **PostgreSQL :** Il s'agit d'un SGBD, son principal point fort est qu'il est gratuit.

→ **RAID :** Cette technologie permet de garantir la redondance des données, il existe différents types de raids.

→ **RAM :** C'est la mémoire vive de l'équipement, elle permet un traitement rapide des actions de l'utilisateur.

→ **Routeur / Router :** Équipement qui permet à un flux de données de changer de réseau.

→ **SFP :** Module permettant de passer d'une connectique à une autre, par exemple, de fibre optique à RJ-45.

→ **SGBD :** Il s'agit d'un logiciel permettant l'administration des bases de données

→ **SIE :** C'est le nom du réseau informatique d'entreprise.

→ **SII :** Il s'agit du réseau industriel de la plateforme.

→ **Snapshot :** Il s'agit d'une « photo » de sauvegarde d'une machine permettant la restauration de cette dernière.

→ **SNMP :** Il s'agit d'un protocole de communication qui permet aux administrateurs réseau de gérer les équipements du réseau.

→ **Split-Brain:** Scénario dans lequel un système d'information possède plusieurs maîtres désynchronisés menant en conséquence à une incohérence des données.

→ **SQL :** Langage structuré permettant d'interroger des bases de données

→ **SVM / CVM :** il s'agit d'une machine virtuelle Nutanix permettant la gestion des autres machines virtuelles d'un nœud.

→ **Synchrone :** Il s'agit d'une technologie synchronisée, c'est-à-dire qu'à chaque instant, les données sont cohérentes.

→ **Trunk :** Technologie permettant à un lien réseau de faire passer des flux de données de différents réseaux.

→ **VLAN :** Il s'agit d'un réseau virtuel.

→ **VM :** Il s'agit d'une machine non physique qui va virtualiser un équipement informatique, le plus souvent un serveur ou un ordinateur.

→ **VMware :** Entreprise spécialisée dans les solutions de virtualisation.

→ **VPN :** Il s'agit d'un réseau privé virtuel sécurisé permettant de chiffrer les données.

Table des matières

Table des illustrations

Table des tableaux

Introduction

À l'issue de mon titre de « Concepteur en Architecte Informatique » effectué sein du CNAM, mon désir de poursuivre mes études m'a naturellement dirigé vers le diplôme d'ingénieur IRSM dispensé par le CNAM. Souhaitant par la même occasion continuer mon avancée dans le monde du travail, j'ai effectué mes dernières unités d'enseignement (UE) en cours du soir afin de ne plus avoir à interrompre ma période en entreprise.

C'est Stéphane Lefebure et Frédéric Delgrange, respectivement « Chef de projet de déploiement des solutions cybersécurité » et « Chef du service informatique » qui m'ont contacté afin de me proposer un poste au sein de Total.

Cette période de travail en entreprise a été plus que bénéfique pour moi. Au cours de ces deux années au sein de TotalEnergies, j'ai vraiment eu le temps de m'intégrer dans le monde du travail et surtout à l'équipe à laquelle j'étais rattaché.

Tout en acquérant de nouvelles compétences, j'ai aussi eu l'occasion de partager les miennes avec mon équipe, notamment avec les notions théoriques vues lors de mes sessions de cours.

J'ai très vite pu évoluer dans mon poste d'administrateur systèmes et réseaux, en commençant par de petits projets pour me familiariser aux coutumes de l'entreprise, jusqu'à de plus gros projets comme celui qui sera détaillé dans ce présent document.

Dans un souci de confidentialité, certaines informations présentes dans ce mémoire ont été volontairement altérées ou supprimées, permettant ainsi sa diffusion publique.

Le projet que j'ai choisi de présenter sous la forme de ce document représente la synthèse de mes deux années au sein de la compagnie TotalEnergies. Il s'agit d'une virtualisation complète du système d'information en partant d'une architecture dépassée depuis déjà plusieurs années.

Ce projet étant très conséquent et impactant, possède la qualité d'englober beaucoup de technologies que ça soit dans le domaine du système, du réseau ou encore de la sécurité informatique ; aussi, ce dernier m'a permis d'approfondir et de

mettre en œuvre mes connaissances en gestion de projet par le biais de la gestion d'équipe, de calendrier et même de budget.

La plateforme de Grandpuits-Gargenville est un environnement de travail particulier ; en effet, il s'agit d'une plateforme pétrolière qui est donc, par conséquent, soumise à la « Directive Seveso », signifiant qu'il s'agit d'un site industriel présentant des risques d'accident majeurs.

Du fait de cette particularité, l'informatique présente à Total est soumise à des réglementations particulières en matière de cybersécurité. Cet environnement de travail rend alors chaque tâche informatique beaucoup plus complexe qu'elle ne le serait dans une entreprise standard, impactant alors par conséquent le projet de virtualisation.

Ce présent document sera sectionné en plusieurs parties ; dans un premier temps, je présenterai de manière détaillée la compagnie TotalEnergies, et plus précisément mon environnement de travail.

Dans une seconde partie, je développerai les problématiques que soulève le projet de virtualisation de la plateforme de Grandpuits-Gargenville, puis dans une troisième section, je décrierai les solutions proposées ainsi que leurs mises en œuvre. Puis, dans un quatrième chapitre, il y sera présenté les résultats, qu'ils soient positifs ou négatifs toujours dans un but de processus d'amélioration continue.

Enfin, je terminerai ce mémoire par une conclusion qui nous permettra d'observer les résultats dans un cadre plus large ; puis, d'observer les possibilités d'évolution qui pourraient se présenter et enfin, de faire une introspection sur ce que j'ai pu apporter à ce projet.

1/ Présentation de l'entreprise

1.1/ Vue d'ensemble

1.1.1/ Gouvernance

TotalEnergies est un acteur majeur de l'énergie, qui produit et commercialise des carburants, du gaz naturel et de l'électricité bas carbone. L'ambition de la compagnie TotalEnergies est de devenir le major de l'énergie responsable et de renforcer sa présence dans les énergies renouvelables grâce au solaire et aux bioénergies.

La société met un point d'honneur à respecter ses cinq valeurs définissant son identité qui sont :

- La sécurité
- Le respect de l'autre
- L'esprit pionnier
- La force de la solidarité
- Le goût de la performance

De toutes ces valeurs, l'une d'entre elles est le point essentiel pour TotalEnergies ; en effet, la compagnie est intransigeante en matière de sécurité. L'exploration, la production ainsi que le raffinage du pétrole sont des activités à haut risque, la société se doit d'être exemplaire en matière de sécurité.

TotalEnergies est, depuis 2020, une société européenne (SE) productrice de multiénergies comme le pétrole, les biocarburants, le gaz ainsi que le renouvelable et l'électricité. L'entreprise possède de nombreuses installations partout dans le monde que ça soit des dépôts pétroliers, des fermes solaires comme dans le désert californien, des stations essence ou encore des raffineries de pétrole et biocarburants.

En France, TotalEnergies possède cinq raffineries :

→ La raffinerie de Normande en baie sur Seine
→ La raffinerie de Donges dans l'estuaire de la Loire
→ La raffinerie de Feyzin en bordure du Rhône
→ La raffinerie de Provence à la Mède
→ La raffinerie de Grandpuits en Seine-Et-Marne

Le siège social de la compagnie se situe à Paris La Défense, communément appelé la « Tour Total » ou encore « La Coupole ».

TotalEnergies, en son sein, se divise en cinq branches, chacune d'entre elles se voit responsable d'un secteur :

→ **Exploration-Production :** secteur qui va permettre le forage du pétrole dans le sol et la récupération du pétrole brut à l'aide de derricks.

→ **Gas, Renewables & Power** : secteur des nouvelles énergies et bioénergies.

→ **Raffinage-Chimie :** secteur où sont placées les raffineries, c'est là qu'on transforme le pétrole brut en produits destinés à la revente.

→ **Marketing & Services :** secteur de la vente et du marketing.

En plus de ces secteurs, il existe différentes divisions responsables de l'innovation, des finances ou encore de la responsabilité du personnel. L'organigramme complet de la compagnie peut être consulté en annexe de ce présent document (*cf. : Organigramme complet*).

Enfin, la compagnie compte plus de 100 000 employés dans plus de 130 pays, ce dernier est présent majoritairement sur les continents européen et africain cependant, il possède aussi des installations aux Amériques, Moyen-Orient et Asie.

Figure 1 - Production d'hydrocarbures par continent

1.1.2/ Historique

La compagnie TotalEnergies fut créée en 1924 par Ernest Mercier. À l'époque, la compagnie ne produisait que du pétrole au Moyen-Orient. Au fil des années, cette dernière a diversifié ses activités en se positionnant sur les secteurs du gaz, du raffinage pétrochimique, de la distribution de produits pétroliers, du solaire, des bioénergies ainsi que de l'électricité.

L'historique ci-dessous répertorie les étapes majeures que l'entreprise a passées depuis sa création jusqu'à aujourd'hui.

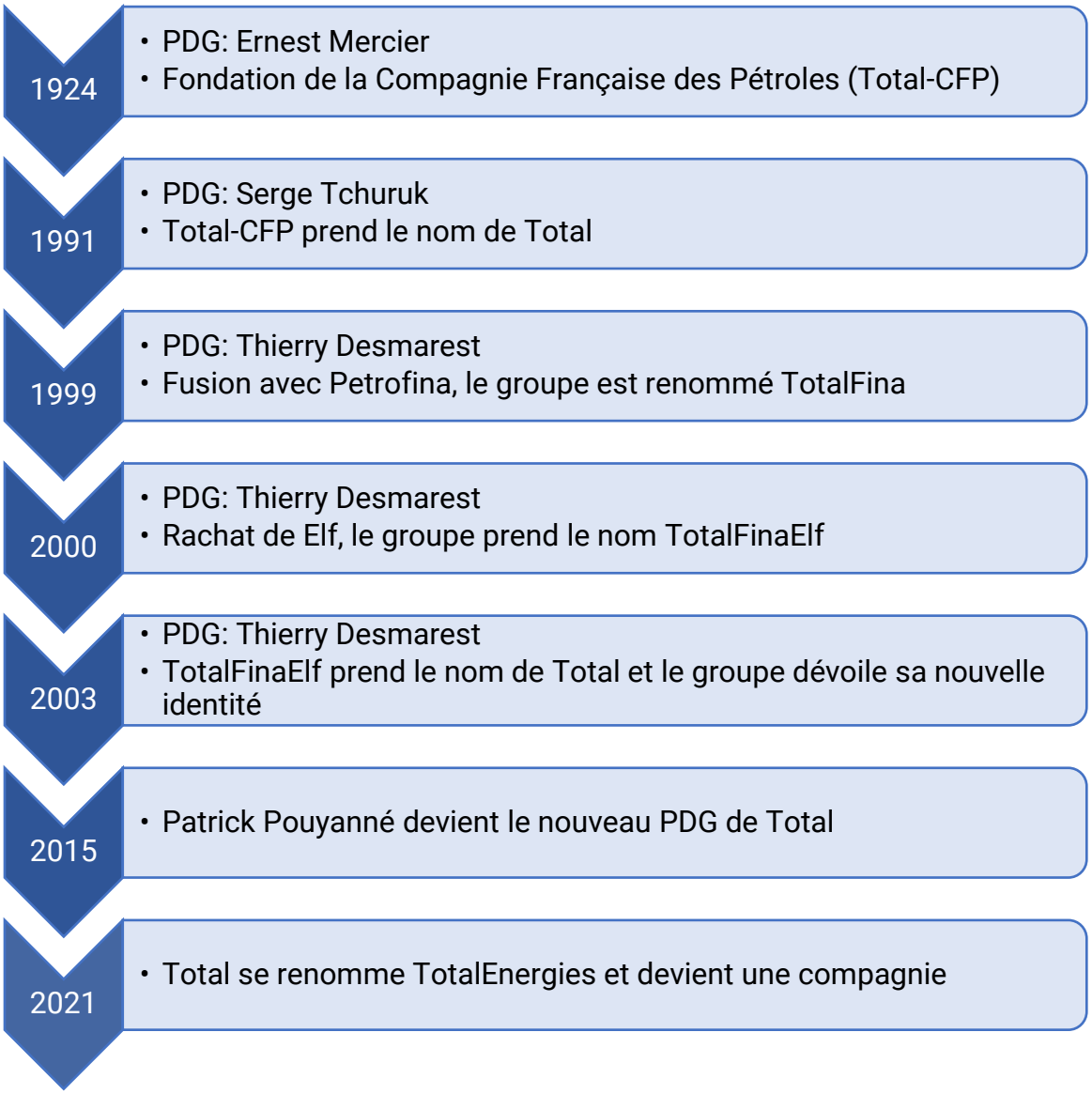


Figure 2- Historique de TotalEnergies

1.2/ Statistiques

1.2.1/ Chiffre d'affaires

Bien que Total possède de nombreuses activités lucratives, elle génère majoritairement son chiffre d'affaires par l'exploration et la production du pétrole.

Chaque jour, c'est environ 2,8 millions de barils de pétrole qui sont produits, un baril équivaut à 160 litres en termes de volume. Par cette génération de barils, Total a pu atteindre un chiffre d'affaires avoisinant les 200 milliards d'euros en 2019.

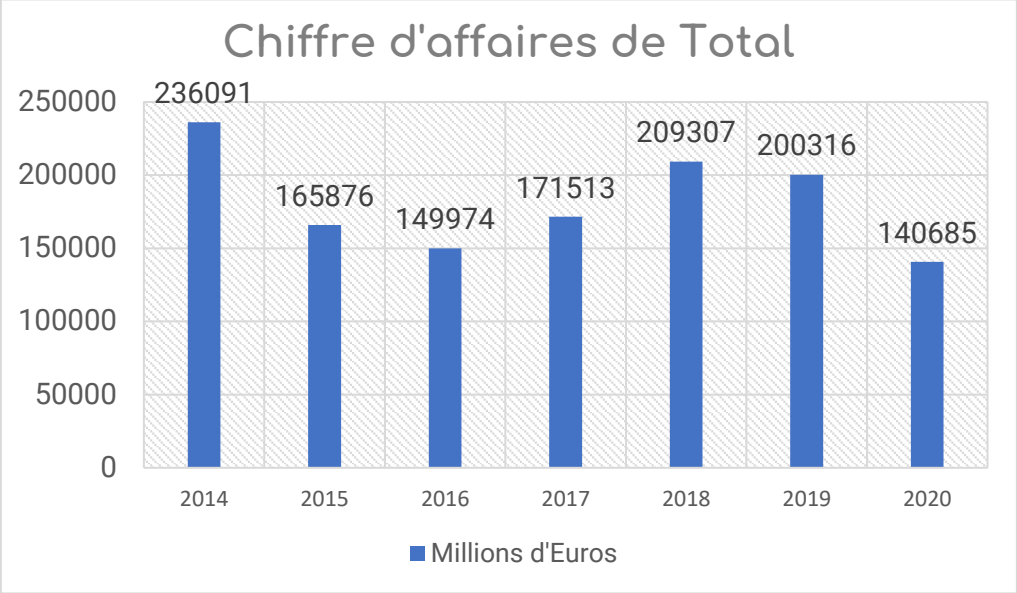


Figure 3 - Graphique du chiffre d'affaires de Total sur 7 années

Nous pouvons constater la chute du chiffre d'affaires de 2020 étant à environ 140 milliards d'euros, soit une perte de presque 60 milliards d'euros. Cette descente est majoritairement due à la crise de la Covid-19, réduisant drastiquement la consommation de pétrole des citoyens français.

En effet, en moyenne, Total génère 50 milliards d'euros par trimestre, cependant, si nous observons les comptes de l'année 2020, la moyenne trimestrielle varie de 44 milliards d'euros à 33 milliards d'euros, avec une chute majeure à 25 milliards d'euros lors du second trimestre de 2020 qui correspond au premier confinement strict imposé par le gouvernement.

1.2.2/ Activité de raffinage

Une autre activité participant de TotalEnergies est le raffinage du pétrole brut. Raffiner ce dernier permet la transformation en plusieurs produits qui peuvent par la suite être commercialisés.

Dans un premier temps, le pétrole subit une distillation atmosphérique, permettant de séparer ses différends, à savoir gazeux, liquide ou solide.

→ Les gaz de propane et de butane sont obtenus après la distillation du pétrole brut au même titre que le kérosène.
→ Les essences et le gasoil sont le résultat d'une stabilisation, puis d'un hydrotraitement du pétrole brut après la distillation atmosphérique.
→ Le soufre, composant toujours présent lors du raffinage du pétrole

Dans une optique de n'effectuer aucun déchet évitable, les ressources inexploitables après la distillation du pétrole subissent une distillation sous vide, permettant la transformation en d'autres composants :

→ Le fioul, qui est un produit lourd, en déclin du fait de son empreinte carbone importante.
→ Le bitume, il s'agit du dernier produit créé à partir des résidus du pétrole brut, il est utilisé pour la construction des routes.

Le détail complet des différentes étapes et processus du raffinage est disponible en annexe (*cf. : Schéma complet du raffinage*).

Par la vente de ces différents produits, le raffinage contribue à l'augmentation du chiffre d'affaires.

1.2.3/ Perspectives de reconversion

Depuis quelques années, partout dans le monde, l'écologie semble devenir de plus en plus majeure dans l'inconscient collectif des populations. Les entreprises cherchent à montrer leur faible impact carbone sur notre atmosphère par le biais de nouvelles stratégies marketing.

Certaines de ces sociétés en ont fait leur force de vente, comme Elon Musk et ses voitures Tesla, acteur majeur de l'électrique ; d'autres entreprises ont cependant échoué dans cette transition vers l'écologie, comme The Coca Cola Company et son « Coca-Cola Life » qui devait être meilleur pour la santé, plus respectueux de l'environnement et permettre à l'entreprise de passer au vert.

TotalEnergies, souffrant de la réputation du pétrole, souhaite montrer les efforts mis en œuvre pour réduire son impact carbone. En 2016, le président-directeur général (PDG) Patrick Pouyanné annonce la création d'une branche d'activité en énergies renouvelables permettant à l'entreprise de faire un grand pas dans ces dernières.

En 2020, la société transforme sa raffinerie de pétrole située à Grandpuits, arrêtant ainsi le raffinage pétrolier pour la production de biocarburants ainsi que des bioplastiques à base de sucre. De plus, le site disposera aussi d'une activité de recyclage chimique des plastiques.

En 2021, la société Total se renomme en TotalEnergies et change de logo dans une logique de communication sur la diversification de ses activités ainsi que l'augmentation de la production des énergies renouvelables.

Figure 4 - Différents logos de TotalEnergies

1.3/ La plateforme de Grandpuits–Gargenville

1.3.1/ Contexte géographique

Au sein de TotalEnergies, j'étais situé à la Plateforme de Grandpuits-Gargenville, plus précisément à la raffinerie de Grandpuits, en Seine-et-Marne. Le site de Gargenville est une ancienne raffinerie devenue un dépôt de pétrole.

Les deux sites sont indissociables du fait que la raffinerie de Grandpuits est alimentée en pétrole brut par un pipeline au départ du Havre, ce pipeline est piloté par le site de Gargenville, c'est-à-dire que c'est à cet endroit géographique qu'on choisit la nature du produit envoyé vers la raffinerie de Grandpuits. Il peut s'agir de pétrole brut, de carburants ou de sondes permettant son nettoyage ; il est aussi possible d'inverser le sens du pipeline et d'envoyer différents types de produits de Grandpuits vers Gargenville.

Cette indissociabilité des deux sites s'observe aussi dans l'informatique, car ces derniers ne forment qu'un seul parc informatique réparti géographiquement, complexifiant ainsi le système d'information. Ainsi, bien que situé la majeure partie de mon temps à Grandpuits, il était possible que j'aie besoin de me rendre à Gargenville pour certaines missions.

Figure 5 - Schéma du Pipeline d'Île-De-France (PLIF)

En 2019, un défaut sur ce pipeline provoquera sa rupture qui entraînera une fuite de 900m³ d'hydrocarbures dans les champs de Autouillet et Boissy-sans-Avoir. Cet évènement précipitera l'arrêt ainsi que la reconversion de la plateforme en 2020.

1.3.2/ Détail

Le site de Gargenville, reconverti en dépôt pétrolier, emploie 43 personnes. Comme dit précédemment, la gestion du PLIF permettant l'apport de ressources à Grandpuits est assurée par Gargenville ; les deux sites travaillent en harmonie.

Le site de Grandpuits quant à lui emploie environ 500 personnes titulaires ainsi que quasiment le même nombre de prestataires. La raffinerie est un site beaucoup plus conséquent que Gargenville, cette dernière traite 4,9 millions de tonnes de pétrole brut par an ; il s'agit cependant de la plus petite des raffineries de TotalEnergies en France.

Géographiquement, la raffinerie se situe à l'adresse « Zone d'activité Total, D619, 77720 – Grandpuits-Bailly-Carrois », elle a été construite au milieu des champs, loin des villes dans un but de sécurité et de qualité de vie pour les habitants.

Figure 6 - Raffinerie de Grandpuits

Le site étant classé « Seveso », il est soumis à d'importantes directives en matière de sécurité ; en effet, effectuer une action de changement requiert dans la majorité des cas un processus d'analyse et de validation de la demande.

L'importance de la sécurité se ressent aussi dans l'organisation de l'informatique, tant sur l'architecture de cette dernière que sur la formation des équipes du service informatique.

1.4/ Organisation de l'informatique

1.4.1/ Contexte

Au sein de la plateforme, il existe une multitude de réseaux différents qui peuvent et sont cloisonnés logiquement et physiquement.

Les différents réseaux ont chacun une utilité particulière, le cloisonnement de ces réseaux permet d'y appliquer différentes politiques de sécurité ou de traitement.

Dans un premier temps, le réseau « DMZ », il s'agit d'une zone démilitarisée (DMZ), tous les flux qui passent d'un réseau à un autre ou qui arrivent d'internet doivent passer par ce réseau avant d'atteindre les multiples réseaux de la plateforme. C'est un réseau qui sert de barrière de sécurité, en cas d'attaque par internet, il est impossible d'accéder directement aux réseaux internes.

Ensuite, le réseau « Partenaires », c'est le réseau où sont hébergés les équipements des entreprises externes à Total qui travaillent sur site. Il permet de ne pas avoir à appliquer certaines règles de sécurité rendant l'implémentation d'équipements d'entreprises externes compliqués comme des box internet.

Enfin, le réseau « Sécurité », c'est ici que sont adressés les équipements de sécurité, comme les caméras, les détecteurs de mouvement, les lecteurs de badges ou encore les serveurs concernant la sécurité.

Cependant, il reste encore deux réseaux, beaucoup plus importants que les précédents, il s'agit des réseaux « Industriel » et « Entreprise. Ces derniers, bien que séparés, sont étroitement liés, ce qui rend la tâche de les isoler correctement les uns des autres difficile.

1.4.1/ Réseau d'entreprise

Le réseau d'entreprise, ou Système d'Information d'Entreprise (SIE), est l'appellation donnée au réseau qui permet l'accessibilité à internet ainsi qu'à l'informatique nécessaire aux différents services présents sur la plateforme.

Du fait de son exploitation par du personnel non-informaticien, ainsi que la possibilité d'accès à Internet, ce réseau, bien que sécurité, ne doit en aucun cas avoir un quelconque contact logique ou physique avec un autre réseau de la plateforme.

En effet, ce réseau étant le plus gros de la plateforme, que ça soit en termes de taille ou de nombre d'utilisateurs, il est, par conséquent le plus risqué ; c'est pourquoi il se doit d'être entièrement isolé des autres réseaux qui peuvent être plus sensibles.

Il n'est pas rare de voir un utilisateur brancher une clé USB infectée ramenée de la maison ou télécharger un fichier corrompu sur internet. Bien qu'il existe de nombreux dispositifs de défense assurant la sécurité du réseau, il s'agit, en théorie, du réseau avec le plus de probabilités d'être compromis.

1.4.2/ Réseau industriel

Le réseau industriel, ou Système d'Information Industriel (SII) concerne des équipements importants puisqu'il s'agit du réseau permettant le pilotage de la plateforme. Cette architecture possède des serveurs et ordinateurs dédiés pour les mesures ou le contrôle des vannes de la plateforme ainsi que des automates et analyseurs.

Par son contexte, ce réseau industriel est soumis à beaucoup de règles de sécurité informatiques. En effet, il n'y a pas d'accès à internet, seul le personnel autorisé peut y accéder et ce dernier est sensibilisé sur les risques informatiques. Il y a aussi différentes technologies informatiques utilisées afin d'assurer la sécurité.

De manière générale, il est très important de respecter la séparation des réseaux pour une sécurité optimale, d'ailleurs, en matière de sécurité des réseaux, la compagnie TotalEnergies a choisi d'appliquer les recommandations de l'Agence Nationale de la Sécurité des Systèmes d'Information (ANSSI) pour l'architecture de ses systèmes d'information.

1.4.3/ Hiérarchie de l'informatique

Au sein de la plateforme, le personnel en charge de l'informatique est le service « Systèmes », c'est à ce dernier que j'ai été affecté en tant qu'administrateur réseaux et systèmes. Les diverses missions du service sont :

→ Installer et configurer des équipements réseau de niveau 2 et 3 ainsi que des équipements industriels de type automates.
→ Sensibiliser les utilisateurs sur les risques liés à l'informatique
→ Maintenir le système d'information en bonne condition, implémenter de nouvelles solutions étudiées au préalable pour son amélioration.
→ Assurer l'accessibilité et la disponibilité des réseaux aux utilisateurs de la plateforme
→ Se prévenir des risques liés aux attaques informatiques en implémentant des solutions sécurisées comme des pare-feux, des Virtual Private Network (VPN) ou encore en implémentant les recommandations de l'ANSSI

Le service ne s'occupe pas du développement d'applications ou logiciel internes ainsi que des problèmes applicatifs que peuvent rencontrer les utilisateurs ; en cas de problème sur un ordinateur, les utilisateurs doivent contacter un service Hotline dédié à ces incidents.

Par les différents réseaux présentés précédemment, le service est divisé en deux équipes ; l'une de ces équipes, composée de 5 personnes statutaires gère l'informatique d'entreprise, l'autre équipe, composée aussi de 5 personnes statutaires s'occupe de l'informatique industrielle.

De plus, des prestataires sont aussi amenés à renforcer l'équipe du service au travers de contrats de supports ou bien lors de projets. Bien qu'il existe deux équipes distinctes, il n'est pas rare que certains employés passent d'une équipe à l'autre en fonction des besoins de chacune.

Je fus affecté à l'équipe du réseau d'entreprise, signifiant donc que la majorité de mes missions se passent sur ce réseau. Cependant, un grand projet de changement des systèmes d'information m'a amené à travailler aussi une majeure partie de mon temps sur le réseau industriel.

Au sein du service Systèmes, l'organigramme est simple, tout le monde possède le même statut de salarié, cependant il y a 3 postes qui se démarquent des autres.

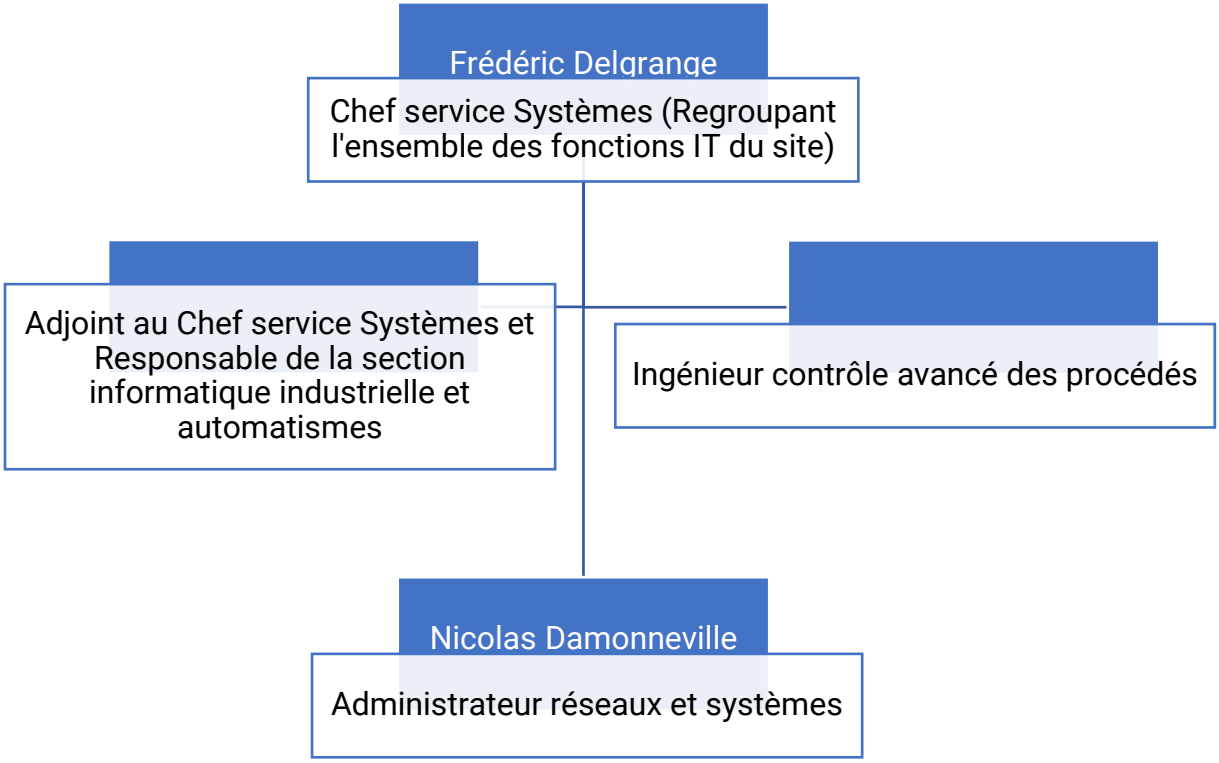


Figure 7 - Organigramme du service Systèmes

Au poste de Chef du service Systèmes se tient M. Frédéric Delgrange, il regroupe l'ensemble des fonctions technologiques du site.

Les deux postes en dessous, à savoir « Adjoint au Chef service Systèmes » ainsi qu' « Ingénieur contrôle avancé des procédés » sont des postes travaillant exclusivement sur le réseau industriel. De plus, l'adjoint au chef est aussi responsable de l'entièreté des automates présents sur la plateforme.

De par mon affectation sur le réseau d'entreprise, les directives de projets me viennent directement de M. Frédéric Delgrange.

2\ Projet d'ingénieur - Virtualisation de la plateforme de Grandpuits-Gargenville

2.1\ Mise en situation

Au sein de la plateforme, les serveurs du réseau SII ainsi que ceux du réseau SIE sont installés physiquement dans deux salles techniques différentes à savoir « ST-16 » et « ST-17 ».

Les serveurs présents dans ces salles ne disposent pas d'espace de stockage, ils ont par conséquent chacun seulement deux disques de stockage pour leur système d'exploitation qui est répliqué en utilisant la technologie Redundant Arrays of Inexpensive Disks (RAID) 1.

Le RAID1 est une technologie permettant à chaque disque d'un serveur de posséder les mêmes données à n'importe quel moment, de ce fait, en cas de panne d'un des deux disques, le serveur reste toujours fonctionnel avec le disque restant et permet ainsi un certain degré de tolérance aux pannes.

En réalité, les données d'exploitation des serveurs sont stockées dans un réseau « Storage Area Network » (SAN). Cette technologie permet de mutualiser les ressources de stockage ; en conséquence, dans nos deux salles techniques, il existe physiquement deux baies SAN qui en représentent une seule virtuelle stockant les données relatives aux serveurs.

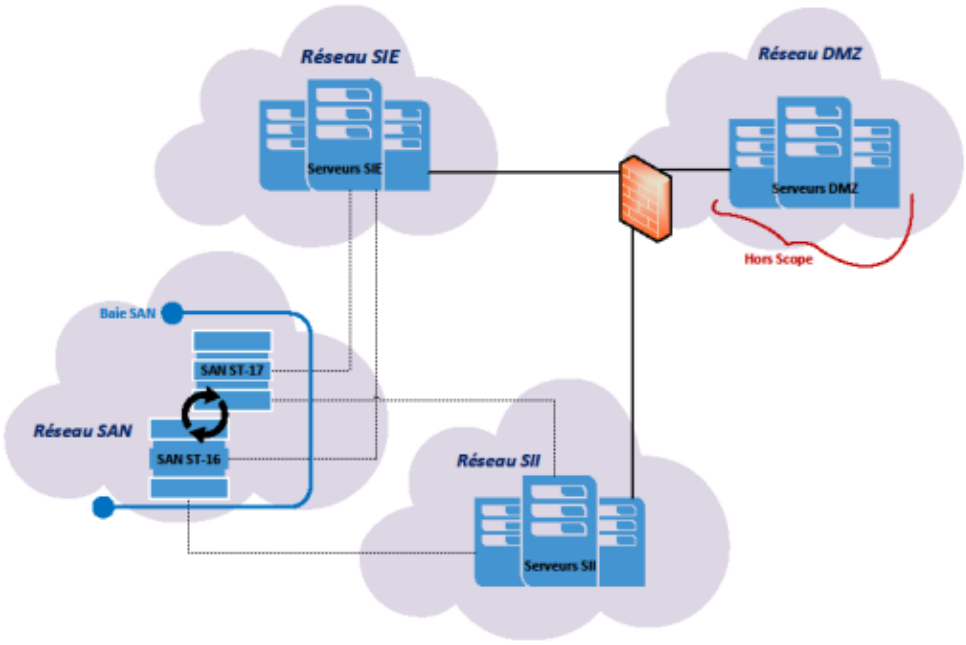


Figure 8 - Réseau SAN

2.2\ Problématique

2.2.1\ Détail

Cette infrastructure réseau présentée précédemment possède plusieurs problèmes, tant sur la sécurité des systèmes d'information que sur son efficacité.

En effet, un des problèmes dans cette architecture est l'inétanchéité des systèmes ; en effet, il est impératif qu'il n'y ait aucun tronc commun entre ces derniers, cependant, bien qu'il y ait un cloisonnement logique qui empêche toute communication entre les réseaux par cette baie SAN, il y a quand même un mode commun physique du stockage des données.

De plus, cette architecture pose un problème de taille, en effet, dans ces deux salles sont stockés environ 80 serveurs, ce qui représente un espace non négligeable de place.

Ce nombre conséquent de serveurs, en plus de la baie SAN et des équipements réseau dans les salles demande une quantité non négligeable de ressources. Chaque serveur est relié par deux alimentations électriques ainsi que deux paires de fibres optiques à la baie SAN, augmentant ainsi considérablement le nombre de câbles réduisant ainsi l'espace dans les salles et les baies informatiques.

Ce nombre colossal de serveurs pose aussi à la fois un problème de place dans la salle, mais aussi de climatisation, les salles étant très petites et fortement remplies, il est difficile de maintenir une température correcte pour le système d'information.

Enfin, en cas de panne ou perte complète d'une des deux salles, il n'existe pas de redondance sur certains serveurs permettant de récupérer ces derniers qui pourraient être détruits.

Tous ces problèmes justifient déjà l'obligation de devoir changer l'infrastructure réseau, cependant, la baie SAN à elle seule soulevait encore un dernier problème majeur qui précipita le lancement du projet.

2.2.2\ La baie SAN

La baie SAN est le cœur de notre architecture ; hébergeant l'espace de stockage de nos serveurs, elle permet de répondre efficacement aux besoins d'évolutivité de la quantité d'espace disque requis.

En effet, un serveur est limité par son nombre d'emplacements disques, l'avantage de la baie SAN est que nous pouvons rajouter des disques en cas de besoin d'espace supplémentaire. Il suffit alors d'augmenter la taille du disque virtuel du serveur concerné par le manque de besoin tout en rajoutant des disques de stockage dans la baise SAN.

Aussi, étant géographiquement placée à deux endroits différents, les données sont dupliquées et disponibles dans chacune de ces baies au cas où l'une d'entre elle venait à être perdue. Cependant, cela n'assure pas la redondance pour les serveurs, en effet, si une salle venait à être détruite, nous aurons toujours les données relatives aux serveurs, il nous faudrait en revanche réinstaller de nouveaux serveurs qui pourront par la suite récupérer les données dans la seconde baie SAN physique.

Sur papier, cette architecture semble bonne, cependant, la baie SAN de TotalEnergies fut installée il y a une quinzaine d'années.

Par sa vieillesse, la baie SAN ne peut plus assurer correctement son rôle, le nombre de disques n'a fait que s'agrandir durant ces années, rapprochant peu à peu le jour où il n'y aura plus d'emplacements libres.

De plus, le type de disque compatible dans la baie SAN n'est même plus commercialisé, laissant alors la baie SAN avec comme disques de rechanges ceux en stock à TotalEnergies.

Enfin, les pannes sont très récurrentes, en été durant les canicules, avec la chaleur naturelle, couplée avec la chaleur de la salle peinant à être refroidie, il y avait entre 1 et 2 disques en panne chaque jour ; cette architecture n'était plus fiable.

2.3\ Gestion du projet

2.3.1\ Organisation

Afin que le projet se déroule sans encombre, il eût fallu passer par une phase d'organisation afin de déterminer toutes les parties prenantes clefs.

La personne mise au statut de chef de projet pour la virtualisation de la plateforme de Grandpuits-Gargenville fut le chef du service Systèmes, M. Frédéric Delgrange ; ce dernier, par son poste possède des connaissances dans tous les domaines auxquels le projet sera lié, que ça soit dans les différents réseaux, la cybersécurité ou encore la partie système.

Pour donner suite à cela, trois personnes virent se greffer à l'équipe, dans un premier temps, l'ingénieur contrôle avancé des procédés qui nous apportera l'expertise nécessaire sur le système d'information SII, notamment sur l'utilisation des différents serveurs, et plus tard, lors de la virtualisation, il pourra nous aider à minimiser les impacts du passage au physique à virtuel.

Dans un second temps, l'ingénieur réseau, ce dernier, par son expertise et sa maîtrise du réseau saura mener à bien la commutation, le routage, le filtrage ainsi que la sécurité de l'architecture mise en œuvre.

Enfin, moi-même, l'administrateur réseaux et systèmes de l'équipe. Ayant de nombreuses connaissances sur l'architecture SIE tant bien réseau que systèmes, je pourrai y apporter des informations et précisions.

De plus, étant inscrit au CNAM, j'ai demandé au chef du service Systèmes si j'avais la possibilité de faire de ce projet mon mémoire d'ingénieur. Frédéric Delgrange ayant accepté cette proposition, il m'a par la même occasion nommé responsable du projet, c'est-à-dire qu'il a laissé le projet entre mes mains et m'a laissé comme missions l'identification ainsi que la gestion des différentes phases du projet que nous détaillerons dans ce présent document.

Enfin, afin d'identifier clairement à quelles parties prenantes clefs je devais faire appel pour les futures tâches du projet, j'ai élaboré une matrice « Responsible, Accountable, Consulted and Informed » (RACI).

Cette matrice permet d'identifier le rôle ainsi que les responsabilités des intervenants au sein de chaque activité liée au projet. Il suffit de détailler, sous la forme d'un tableau, les tâches des projets en ligne et les intervenants en colonne. De ce fait, aux croisements des lignes et colonnes, nous ajoutons une lettre en fonction du rôle de la personne lors de chaque tâche.

Il existe 4 rôles différents dans une matrice RACI :

→ **R :** Signifie « **Responsible** », réalisateur en français, il s'agit de la personne qui travaillera sur la tâche.

→ **A :** Signifie « **Accountable** », approbateur en français, il s'agit de la personne responsable de la tâche, plus précisément, c'est à lui de rendre des comptes sur cette dernière et d'en assumer le résultat.

→ **C :** Signifie « **Consulted** », consulté en français, il s'agit de la personne devant être consultée lors de la réalisation de la tâche. C'est une obligation de consultation et non une possibilité. Ces personnes permettent d'apporter une expertise à la tâche sans pour autant travailler dessus.

→ **I :** Signifie « **Informed** », informé en français, il s'agit de la personne devant être informée du déroulement de la tâche.

Il est possible pour une personne de posséder plusieurs rôles lors d'une tâche, par exemple, une personne peut avoir le rôle de réalisateur et de consulté à la fois.

Aussi, il peut y avoir plusieurs réalisateurs sur la même tâche, cependant, ce n'est pas le cas de l'approbateur. En effet, il ne peut y avoir qu'un seul approbateur par tâche, car plus la responsabilité est partagée, moins il y en a.

	NICOLAS	FREDERIC	INGE. SII	INGE. RESEAUX
Listing des ressources	R	AC	C	I
Définir l'architecture cible	R	AC	C	RC
Définir la méthode de licenciement	R	A	I	I
Rédaction du cahier des charges	R	A	C	C
Publication du cahier des charges	I	AR	I	I
Analyse des offres	R	AR	R	C
Achat de la solution	I	AR	I	I
Analyse réseau SIE	R	AC	I	RC
Analyse réseau SII	R	AC	C	RC
Installation physique des serveurs de virtualisation	R	A	I	I
Achat de commutateurs	C	A	C	R
Installation physique des commutateurs	R	I	I	AR
Configuration des commutateurs	R	C	I	AR
Configuration des routeurs	R	C	I	AR
Gestion des flux pare-feu	R	C	I	AR
Définition des cheminements fibre optique	I	C	C	AR
Raccordement des équipements réseau	R	I	I	AR
Tests de l'architecture réseau	R	I	I	AR
Raccordement des serveurs au réseau	R	A	I	I
Configuration du commutateur virtuel	R	I	I	AR

	NICOLAS	FREDERIC	INGE. SII	INGE. RESEAUX
Tests de connectivité	R	I	I	AR
Importation des images Windows	R	A	I	I
Création des machines virtuelles	R	A	R	I
Création des actions de sauvegarde	R	AC	R	I
Conversion des serveurs physiques à virtuel	R	AR	R	I
Ajout de la supervision	R	A	C	C
Décommission des serveurs	R	A	C	C
Décommission de la baie SAN	R	AR	C	C
Mise à jour des documentations techniques	R	AC	RC	C
Formation des utilisateurs	I	AR	R	I

Tableau I - Matrice RACI

Cette matrice définissant maintenant le rôle de chacune des parties prenantes du projet, il devrait être moins probable de rencontrer des problèmes liés à la gestion du projet.

2.3.2\ Phases

Par son ambition, ce projet demande des connaissances dans plusieurs domaines de l'informatique, comme le réseau, le système, la virtualisation ou encore la sécurité.

C'est pourquoi il est possible de le diviser en plusieurs grandes phases qui demanderont chacune des connaissances différentes le moment venu.

Dans un premier temps, nous devons organiser une phase d'analyse nous permettant de connaitre nos consommations énergétiques actuelles pour nos serveurs ; de ce fait, il sera plus facile de dimensionner notre future architecture, de plus cela nous évitera de faire du sur ou sous-dimensionnement. Toujours dans cette même phase, nous devons définir l'architecture cible que nous souhaitons, c'est-à-dire une solution de virtualisation hyperconvergée. Enfin, nous souhaitons réfléchir aux perspectives d'évolution des systèmes d'information, la solution devra être évolutive.

Ensuite, dans un second processus, nous devons assurer la connectivité de la solution à notre infrastructure. Étant donné que nous souhaitons avoir des clusters répartis géographiquement, il faudra probablement faire passer de nouvelles gaines de fibres dans le sol. La solution sera responsable de la virtualisation d'un grand nombre de serveurs, il serait alors judicieux d'ajouter de nouveaux équipements de routage et de commutation qui seront dédiés à cette infrastructure afin d'assure un haut débit et une meilleure sécurité. Cela signifie alors qu'il y aura toute une étape réseau ayant pour but la modification de notre infrastructure réseau afin d'y intégrer cette nouvelle solution et que, par conséquent, il faudra penser à comment configurer le routage et les flux sur les pare-feux.

Par ailleurs, il y aura une petite phase d'installation physique des équipements réseau ainsi que de la solution, en effet, comme précisé précédemment, les salles techniques sont complètes, il n'y a presque plus de place dans les baies informatiques, cela signifie qu'il faudra probablement enlever des serveurs des baies afin de les mettre temporairement au sol tout en les maintenant fonctionnels le temps de la fin de ce projet.

Après la précédente phase, nous pourrons enfin commencer à virtualiser des machines. Il s'agit d'une étape très importante qu'il faut effectuer avec beaucoup de précautions. En cas de virtualisation d'un nouveau serveur, il n'y a pas vraiment de risques, cependant, ce n'est pas le cas lors du passage au virtuel d'un serveur étant physique. En effet, il existe plusieurs techniques pour passer du physique au virtuel, elles seront détaillées dans ce présent document.

Cependant, bien qu'il existe plusieurs techniques, nous n'avons pas de solution pour ne pas interrompre la communication avec le serveur, c'est-à-dire qu'il y aura forcément une phase où le serveur ne sera pas joignable. De plus, même en faisant une copie complète du serveur physique puis qu'on installe cette copie dans un serveur virtuel, il est possible que certains services et logiciels propriétaires ne fonctionnent plus correctement, ce qui signifiera faire un retour arrière.

Nous profiterons aussi de cette phase de virtualisation pour mettre à jour certains de nos serveurs restés à des versions de Windows très anciennes.

La phase de virtualisation sera accompagnée en parallèle d'une phase de décommission des serveurs physiques au fur et à mesure de leur virtualisation, ce qui permettra de réduire les besoins en climatisation de la salle ainsi que d'augmenter l'espace de stockage dans les baies informatiques. La fin de cette étape sera clôturée par la décommission complète de la baie SAN, signant ainsi la fin de cette architecture.

Bien que l'architecture soit fonctionnelle après l'étape précédente, il reste néanmoins une dernière phase de formation, de mise à jour de documentations, d'axes d'amélioration ainsi qu'un processus de retour d'expérience dans une démarche d'amélioration continue. Une fois ceci terminé, nous pourrons valider la fin du projet.

2.4\ Analyse du besoin

2.4.1\ Ressources utilisées

Le projet de virtualisation de la plateforme Grandpuits-Gargenville a pour but de virtualiser tous les serveurs présents dans les locaux informatiques. C'est-à-dire que nous aurons une machine physique hébergeant plusieurs serveurs virtuellement.

Pour se faire, la première étape est donc de faire un état des lieux du parc actuel pour avoir une vision détaillée des ressources que nous utilisons actuellement. À la suite de ce relevé d'informations, nous serons en mesure de dimensionner correctement l'architecture envisagée.

Précédemment, avec l'architecture SAN, les seules ressources qui nous importaient étaient celles relatives au stockage ; si nous souhaitons passer sur une architecture virtualisant les serveurs, il nous faut prendre en compte plus de paramètres.

En effet, la puissance de calcul est à prendre en compte, car dans l'architecture SAN, chaque serveur possédait son processeur et sa « Random Access Memory » (RAM), le rendant responsable de sa propre puissance de calcul.

En cas de virtualisation, la machine physique doit posséder une banque de puissance de calcul qu'elle allouera de manière dynamique à chaque serveur virtualisé en fonction de ses besoins.

Afin de récupérer les informations concernant la consommation de nos systèmes d'information SII et SIE, j'ai utilisé un logiciel propriétaire s'installant sur un ordinateur qui interrogera pendant 24h les serveurs sur leurs consommations et taille.

Le logiciel se base sur le protocole « Simple Network Management Protocol » (SNMP), ce protocole permet de récupérer des informations en temps réel relatif aux équipements connectés, comme leur température, leur disponibilité, etc.

J'ai donc installé ce logiciel sur deux ordinateurs administrateurs du réseau SII et SIE étant donné qu'il s'agit des seuls ordinateurs ayant un trafic autorisé vers l'ensemble des serveurs.

Grâce à cette analyse, j'ai pu récupérer rapidement les informations qui m'étaient utiles au dimensionnement de l'architecture future, à savoir :

→ Nom du serveur
→ Marque du serveur
→ Système d'exploitation
→ Réseau d'appartenance SII ou SIE
→ Adresse IP
→ Nombre de cœurs CPU
→ RAM
→ Nombre de disques virtuels
→ Capacité utilisée des disques virtuels
→ Capacité libre des disques virtuels
→ Pics d'utilisation
→ Performances d'écriture

Après 24 heures, toutes ces informations sont ensuite relevées dans un tableau récapitulant la consommation des ressources par serveur :

Nom du serveur	Nom de disque	Capacity totale	Capacité libre	Capacité utilisée	IOPS	Pic Disk Throughput	Read/Write
[illegible]	0 C:	67,00 Go	27,00 Go	40,00 Go	9 à 95 %	5,40 Mo/s	52 % / 48 %
[illegible]	1 E: I: J:	1,63 To	1,62 To	8,00 Go	7 à 95 %	3,60 Mo/s	35 % / 65 %
[illegible]	2 F:	600,00 Go	427,00 Go	173,00 Go	11 à 95 %	50,50 Mo/s	90 % / 10 %
[illegible]	3 H: H: G:	800,00 Go	692,00 Go	108,00 Go	0 à 95 %	13,80 Mo/s	97 % / 3 %
[illegible]	0 C:	278,00 Go	182,00 Go	96,00 Go	83 à 95 %	28,60 Mo/s	93 % / 7 %
[illegible]	0 C:	136,00 Go	86,00 Go	50,00 Go	4 à 95 %	6,00 Mo/s	53 % / 47 %
[illegible]	1	1,09 To	1,07 To	20,00 Go	0 à 95 %	0,50 Mo/s	18 % / 82 %
[illegible]	0 C:	67,00 Go	29,00 Go	38,00 Go	19 à 95 %	7,00 Mo/s	1 % / 99 %
[illegible]	1	335,00 Go	324,00 Go	11,00 Go	1 à 95 %	0,00 Mo/s	0 % / 100 %
[illegible]	0 C:	67,00 Go	11,00 Go	56,00 Go	80 à 95 %	10,50 Mo/s	79 % / 21 %

Figure 9 - Tableau de consommation par serveur

Une fois en possession de toutes ces informations, il ne me restait plus qu'à regrouper les serveurs par réseau d'appartenance afin de répondre au besoin de ségrégation des réseaux.

Ainsi, pour les deux réseaux SIE et SII, j'ai édité une feuille récapitulative comme présentée ci-dessous (valeurs non représentatives de la réalité) :

Figure 10 - Feuille récapitulative d'un système d'information

Nous pouvons observer pour ce réseau que l'addition des ressources de tous les serveurs donne 84 cœurs CPU, 168 giga-octets (Go) de RAM ainsi que les performances d'écriture du serveur.

Grâce à ces dernières, nous savons à quel moment un serveur est le plus sollicité et s'il possède assez de puissance de calcul pour compléter ses opérations, de ce fait, nous pouvons facilement identifier les serveurs ayant été sur ou sous-dimensionnés :

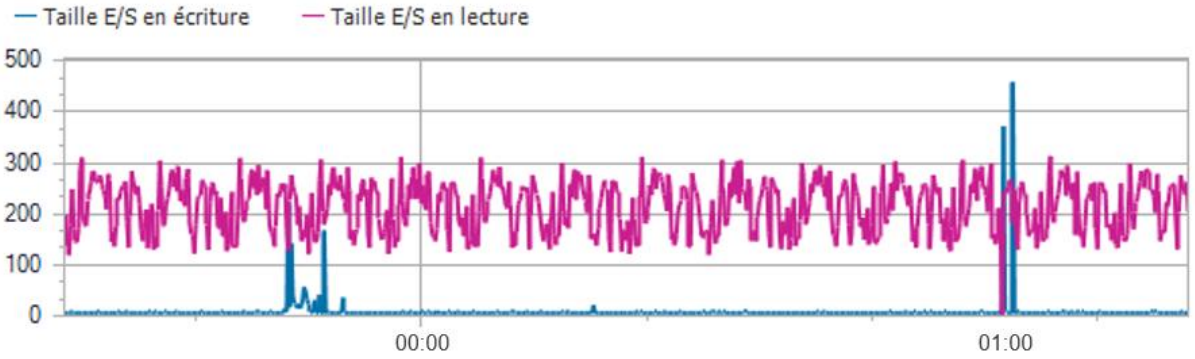


Figure 11 - Pic d'écriture à 01:00 correspondant à l'heure de sauvegarde

En conclusion, nous pouvons observer qu'en grande partie, nos systèmes d'information SII et SIE sont surdimensionnés en RAM avec seulement 15% d'utilisation au contraire de l'espace de stockage qui lui est sous-dimensionné avec seulement environ 5 Téraoctets (TO) restants.

2.4.2\ Architecture envisagée

Une fois le travail d'analyse des ressources utilisées effectué, je me suis penché plus en détail sur l'architecture.

En me basant sur des solutions de virtualisation actuellement en place sur le marché, j'ai élaboré un schéma de principe de l'architecture souhaité. De ce fait, lors de la rédaction future du cahier des charges, mes potentielles offres de prestataires pourront s'inspirer de mes schémas et comprendre ce qui est attendu.

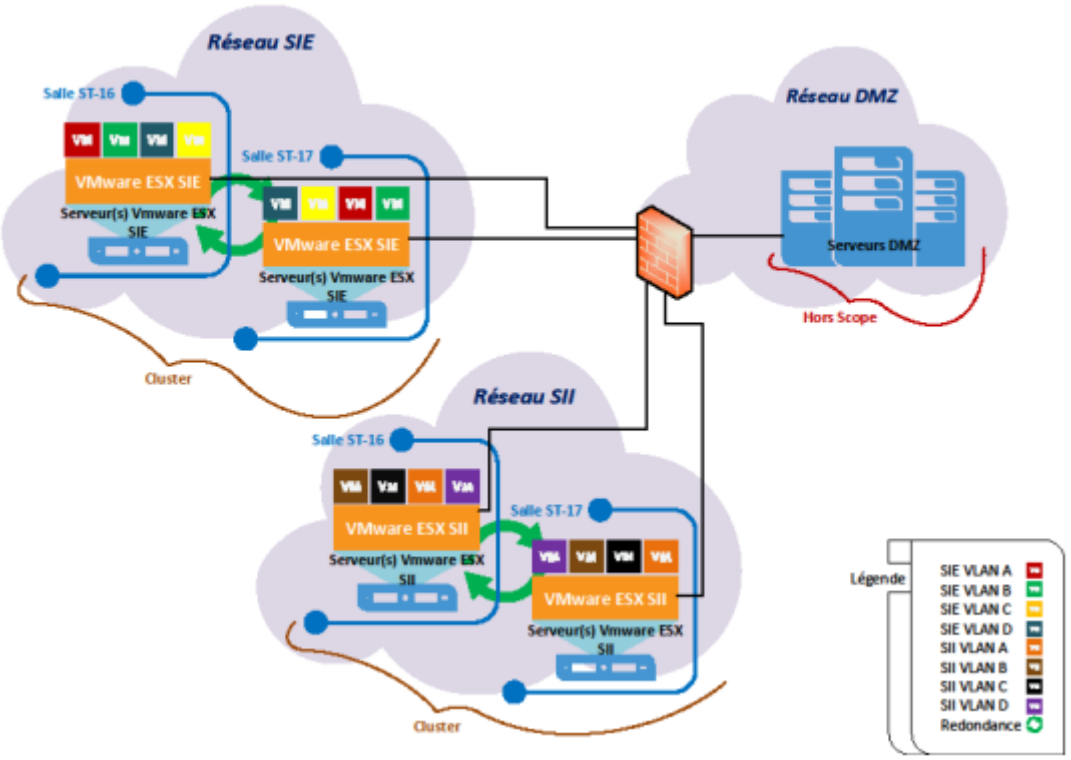


Figure 12 - Schéma de principe de l'architecture souhaitée

Venant en remplacement de l'architecture SAN, deux clusters de deux nœuds d'ESX disposant de leur propre capacité de stockage. Un ESX est une machine physique qui aura pour but d'héberger plusieurs serveurs virtuels, il s'agit d'une solution propriétaire de VMware.

Chaque réseau s'appuiera donc sur un cluster de deux nœuds d'ESX, chacun de ces deux membres sera dans une salle technique différente. Ces machines répliquant leurs données entre elles permettent alors d'héberger indifféremment les serveurs virtuels sur l'une ou l'autre.

Cette nouvelle infrastructure a pour avantage de diminuer de manière conséquente le nombre de machines physiques, ce qui permet de réduire l'espace nécessaire dans les locaux techniques ainsi que les besoins en climatisation et la consommation énergétique.

Aussi, cette architecture facilite la mise en place de plan de reprise d'activité (PRA) et plan de continuité d'activité (PCA). En cas de sinistre, le PRA permet de reconstruire les serveurs en leur affectant les données répliquées et ainsi de redémarrer les applications très rapidement.

Enfin, elle permet d'assurer que les systèmes d'information SII et SIE sont complètement cloisonnés et séparés physiquement avec aucun mode commun ; en effet, les clusters sont raccordés à leur réseau respectif et séparés par un pare-feu.

En conclusion, cet exemple de solution nous permet de répondre à toutes les problématiques précédentes que soulevait le réseau SAN.

Après confirmation de l'unanimité de l'architecture auprès des autres parties prenantes de ce projet, je possédais toutes les informations nécessaires à la rédaction d'un cahier des charges ; c'est-à-dire, la quantité de ressources informatiques utilisées par nos systèmes d'information ainsi qu'un exemple de solution de virtualisation attendue.

2.4.3\ Cahier des charges

Après tout mon travail d'analyse, j'ai rédigé un cahier des charges comportant les informations nécessaires aux potentiels prestataires ; c'est-à-dire les ressources consommées par nos serveurs actuellement ainsi qu'un souhait d'architecture pour le site de Grandpuits.

Nous avons aussi précisé que nous souhaitons une architecture fonctionnelle sur 10 années, il ne faut pas que les prestataires nous présentent une solution remplissant à l'octet près notre consommation actuelle, autrement, nous serions dans l'incapacité de faire évoluer nos systèmes d'information.

Aussi, dans la partie présentation d'entreprise, j'ai précisé que les sites de Grandpuits et Gargenville étaient indissociables, et ce, même pour l'informatique. En effet, comme pour Grandpuits, j'ai effectué une analyse des ressources utilisées à Gargenville, cependant, je n'ai pas présenté de solution exemple.

Gargenville étant beaucoup moins conséquent en termes de serveurs, c'est-à-dire moins d'une quinzaine, j'ai laissé la proposition de la solution libre au prestataire, de plus, l'architecture de Gargenville est en état moins critique que celle de Grandpuits pour la simple et bonne raison qu'elle ne repose pas sur le réseau SAN.

La solution de clusters d'ESX ne semblait pas être adaptée pour Gargenville, les coûts étaient beaucoup trop élevés et n'ayant pas à ma connaissance toutes les architectures système, j'ai préféré laisser le choix libre aux répondants.

J'ai aussi ajouté dans ce cahier les contacts directs des différents intervenants TotalEnergies au projet dans l'optique où les prestataires avaient des questions.

Figure 13 - Interlocuteurs techniques de TotalEnergies

2.4.4\ Licenciement de l'architecture

2.4.4.1\ Windows

Au sein de la plateforme de Grandpuits-Gargenville, à de rares exceptions près, tous les serveurs utilisent le système d'exploitation Windows sous différentes distributions.

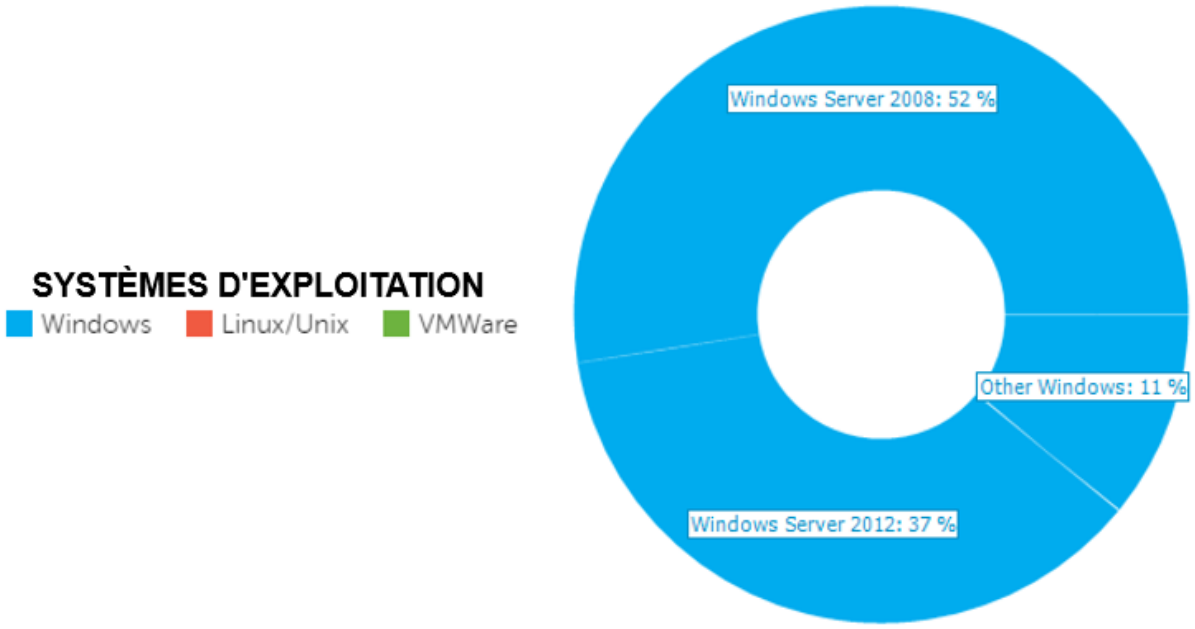


Figure 14 - Différentes distributions de Windows Server présentes

Dès lors que nous passons à des serveurs au virtuel, nous sommes confrontés à un problème de licenciement. En effet, le remplacement de l'infrastructure nous oblige à nous poser la question de la migration des licences « Windows Server » physiques à « Windows Server » virtuel et également comment gérer la virtualisation de serveurs supplémentaires.

Lorsque nous nous penchons sur les méthodes de licenciement proposées par Windows dans un environnement virtualisé, nous avons le choix entre deux solutions :

→ Licenciement au nombre de serveurs virtuels

→ Licenciement au nombre de cœurs physiques

Le licenciement au nombre de serveurs virtuels signifie qu' un serveur est égal à une licence ; si je virtualise un serveur Windows 2008, je dois avoir une licence Windows 2008 au minimum.

Cette solution comporte beaucoup d'inconvénients et ne semble pas adaptée dans notre cas, en effet, il nous faudrait acheter aux alentours de 80 licences et si nous souhaitions virtualiser de nouveaux serveurs nous devrions acheter de nouvelles licences.

Le licenciement au nombre de cœurs possède lui aussi des inconvénients, nos ESXs sont équipés d'un certain nombre de cœurs CPU, si nous souhaitons virtualiser un seul serveur, il faut que l'ESX qui virtualise ce serveur possède une licence pour chacun de ses cœurs.

Cette solution n'est pas adaptée aux architectures souhaitant virtualiser peu de serveurs, mais dans notre cas, cela semble plus raisonnable du fait de notre nombre conséquent de serveurs.

Bien que le choix semble se concrétiser pour le licenciement par nombre de cœurs, j'ai quand même demandé un devis à InSight, il s'agit de la société prestataire de TotalEnergies responsable des contrats de licences.

En résultat, le licenciement au nombre de cœurs a été la solution semblant la plus rentable. En effet, nos ESXs possèderont des cœurs physiques très puissants qui pourront virtualiser des centaines de serveurs, il est donc beaucoup plus bénéfique de licencier tous les cœurs des ESXs plutôt que chaque serveur virtuel.

De plus, en choisissant cette solution, nous pourrons agrandir notre environnement virtuel sans coûts supplémentaires dans les années à venir.

2.4.4.2\Oracle

Oracle est un Système de Gestion de Bases de Données (SGBD), il est utilisé sur 4 serveurs qui sont amenés à être virtualisés, cependant, le licenciement des bases de données d'Oracle est différent de celui de Windows.

Oracle propose dans un environnement virtuel deux solutions de licenciement :

→ Licenciement au nombre d'utilisateurs

→ Licenciement au nombre de cœurs

Un licenciement au nombre d'utilisateurs signifie qu'il faut payer une licence pour chaque personne utilisant les données de la base de données (BDD). Par exemple, si un panneau télévisé projette des données relatives à la BDD, une personne lisant ce panneau serait alors considérée comme un utilisateur. En effet, Oracle demande l'identification nominative de tous les utilisateurs accédant à la base. Cette identification est impossible tant le nombre d'utilisateurs est conséquent.

La précédente solution étant impossible à implémenter dans notre système d'information, le seul choix restant est le licenciement au nombre de cœurs.

Cependant, cette solution n'est pas non plus envisageable, en effet, il nous faudrait de nouveau acheter des licences pour l'entièreté de nos cœurs physiques alors que nous ne virtualiserons que 4 serveurs qui consommeraient à peine 1 voire 2 cœurs physiques. Oracle ne pouvant pas être sûr que nous ne virtualisons que 4 serveurs à tout instant, nous sommes dans l'obligation de licencier toute la solution.

En conclusion, aucune des méthodes de licenciement ne conviendrait à notre nouvelle architecture, c'est pourquoi un nouveau projet visant à convertir les bases de données d'Oracle à PostgreSQL a été lancé en parallèle sous la responsabilité d'une autre équipe.

En conclusion, après cette conversion, nous n'aurons plus de problèmes de licenciements.

2.4.5\ Appel d'offres

Par suite de la publication du cahier des charges, seulement deux offres respectaient nos conditions d'architecture, dans cette présente partie, nous allons détailler ces offres qui nous proposent deux solutions ne reposant pas sur les mêmes technologies.

2.4.5.1\ Architecture maître-esclave

Avant de pouvoir détailler les offres, un point sur le fonctionnement des architectures de virtualisation semble obligatoire.

De manière générale, lorsqu'un cluster d'équipement travaille ensemble, afin d'éviter des conflits dans la gestion des données, il y a un nœud maître et un nœud esclave. C'est ce qu'on appelle une architecture « Maitre-Esclave », c'est une méthode de fonctionnement très répandue, il existe cependant des solutions avec plusieurs maîtres où est tolérée l'incohérence des données, mais ce ne sera pas notre cas.

Dans une architecture maître-esclave de deux nœuds, l'un d'eux est élu maître tandis que l'autre est élu esclave. Supposons que je souhaite virtualiser un serveur, je vais alors donner la responsabilité de ce serveur virtuel à l'un des deux nœuds, cela signifiera qu'il sera maître de ce dernier et qu'il est donc responsable de sa mise à disposition sur le réseau.

L'esclave quant à lui n'a pas le droit de virtualiser ce serveur virtuel, car il est déjà virtualisé par le maître, sinon, il en résulterait par un doublon de serveur et par conséquent à une perte de communication par suite d'une duplication d'adresse IP sur le réseau. Lorsque le maître rencontre un problème l'empêchant de virtualiser le serveur, comme une panne, l'esclave va recevoir une alerte lui autorisant de virtualiser le serveur dont le maître était responsable.

Il est possible, dans ce type d'architecture de mettre un nœud actif et un nœud passif, ce qui signifie que le nœud actif est alors maître et virtualise l'entièreté des serveurs à lui seul, l'esclave quant à lui attend seulement que le maître rencontre un problème. Cependant, ce type de fonctionnement n'est pas intéressant, nous préférons avoir deux nœuds actifs chacun à la fois maître et esclave de différents serveurs avec toujours un seul maître par serveur ce qui permet alors une répartition de la charge entre les deux nœuds.

2.4.5.2\ Offre TGITS

TotalEnergies Global Information Technology Services (TGITS) est une branche informatique de la compagnie proposant un catalogue de solutions à des projets techniques pour l'ensemble de l'entreprise ; cette dernière est située à Paris, plus précisément au siège.

La solution de TGITS se repose sur la virtualisation Nutanix qui est une entreprise de virtualisation d'infrastructure assez récente sur le marché du virtuel, ce qui explique pourquoi ils sont peu connus comparés à des leaders du marché comme VMware.

La solution proposée se base sur un cluster de deux nœuds pour chaque réseau, cependant, ces clusters sont asynchrones. Un cluster asynchrone signifie que les données des deux nœuds virtualisant les serveurs sont différentes. Si nous voulons prendre un exemple concret, un serveur virtuel nommé « A » pourrait être virtualisé par un des deux nœuds et sauvegardé sous la forme de « Snapshot » sur l'autre nœud. En cas de panne brutale du premier nœud, le second nœud démarre le serveur virtuel « A » cependant il y aura un delta de différence sur les données du serveur.

En effet, du fait que la solution est asynchrone, les snapshots, qui sont des sauvegardes des serveurs virtualisés, sont envoyées à l'autre nœud ne virtualisant pas le serveur à l'instant présent tout les « X » temps. Supposons que nous avons programmé les snapshots toutes les heures, une panne sur le nœud primaire ayant lieu 55 minutes après la précédente snapshot aura comme effet de remettre en ligne le serveur virtuel « A » avec toutes les données perdues des 55 minutes suivant la dernière snapshot sur l'autre nœud.

Cependant, une solution asynchrone possède certains avantages ; en effet, dans un premier temps, ce genre de solutions est beaucoup moins cher qu'une solution synchrone, de plus, les solutions synchrones ont tendance à saturer le trafic réseau.

L'architecture de TGITS est composée de 2 clusters de deux nœuds (ou node en anglais), chaque nœud étant composé de 3 serveurs :

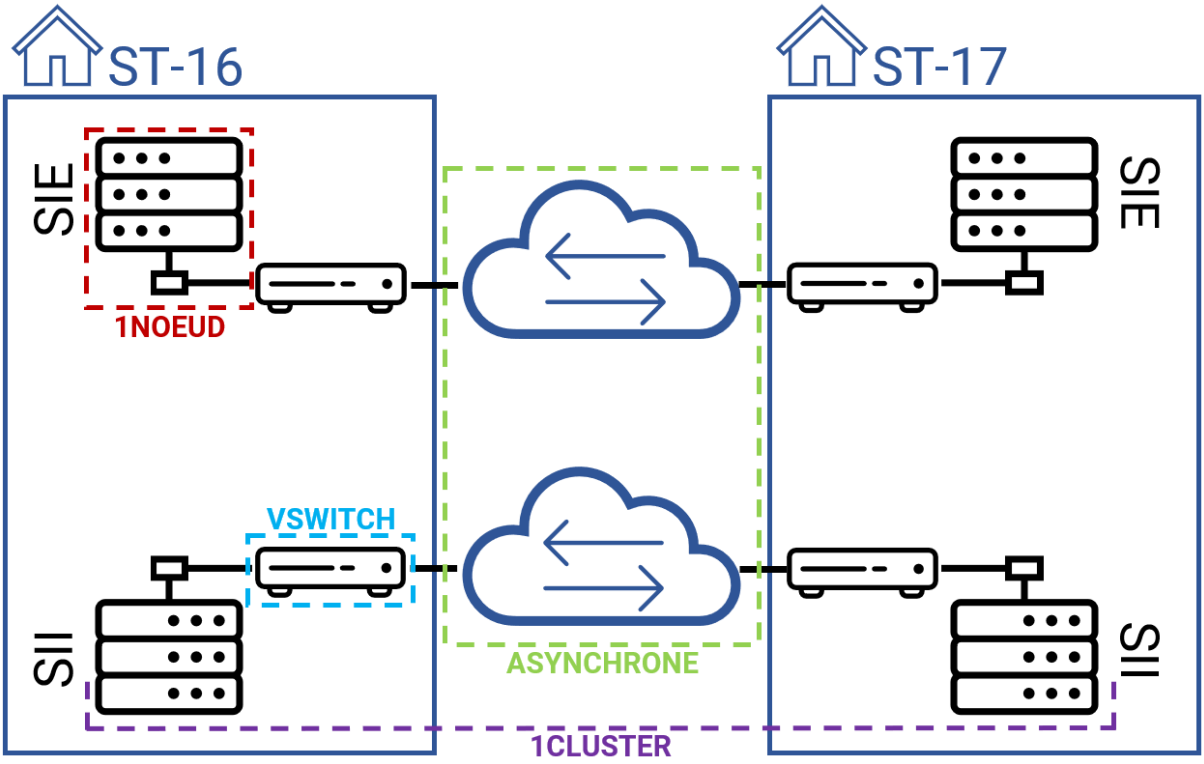


Figure 15 - Architecture TGITS

TGITS ne s'occupe que de nous fournir les nœuds, en ce qui concerne la connectivité au réseau, c'est à notre équipe de choisir une topologie réseau assurant la haute disponibilité, cette dernière sera détaillée dans une prochaine partie du présent document.

Le «Virtual Switch » (vSwitch) est intégré à la solution de virtualisation, il permet à un nœud d'être présent sur différents « Virtual Local Area Network » (VLAN) à la fois sans avoir à posséder plusieurs liens RJ-45 sur une carte réseau différente.

Chaque nœud aura pour mission de virtualiser un certain nombre de « Virtual machines » (VM), chacune d'entre elles utilisera des ressources d'un des serveurs du nœud. En cas de panne d'un serveur au sein d'un nœud, ce dernier redémarre immédiatement la VM localement sur l'un de ses serveurs restants fonctionnels, la localité est prioritaire du fait qu'il n'y a pas de delta de différence dans les données. En cas de panne complète d'un nœud, le nœud dans l'autre salle s'occupe de redémarrer les VM déconnectées du réseau avec un certain delta de différence dans les données.

2.4.5.3\ Offre Antemeta

Antemeta est une entreprise de prestation travaillant souvent avec TotalEnergies, ce sont notamment eux qui s'occupent de nos solutions de sauvegarde sur d'autres infrastructures.

Cette entreprise a aussi répondu à notre appel d'offres par une solution respectant aussi notre cahier des charges cependant, bien différente de la solution proposée par TGITS.

En effet, bien qu'il y ait quelques points communs, la solution de Antemeta est quant à elle une solution synchrone, c'est-à-dire qu'il n'y a pas de delta de différence dans les données relatives aux VM sur chacun des nodes.

Afin d'assurer une solution synchrone, un troisième équipement est nécessaire à l'infrastructure, il s'agit d'un arbitre. Ce dernier va permettre d'apporter un vote supplémentaire sur l'élection du maître actuel de l'architecture.

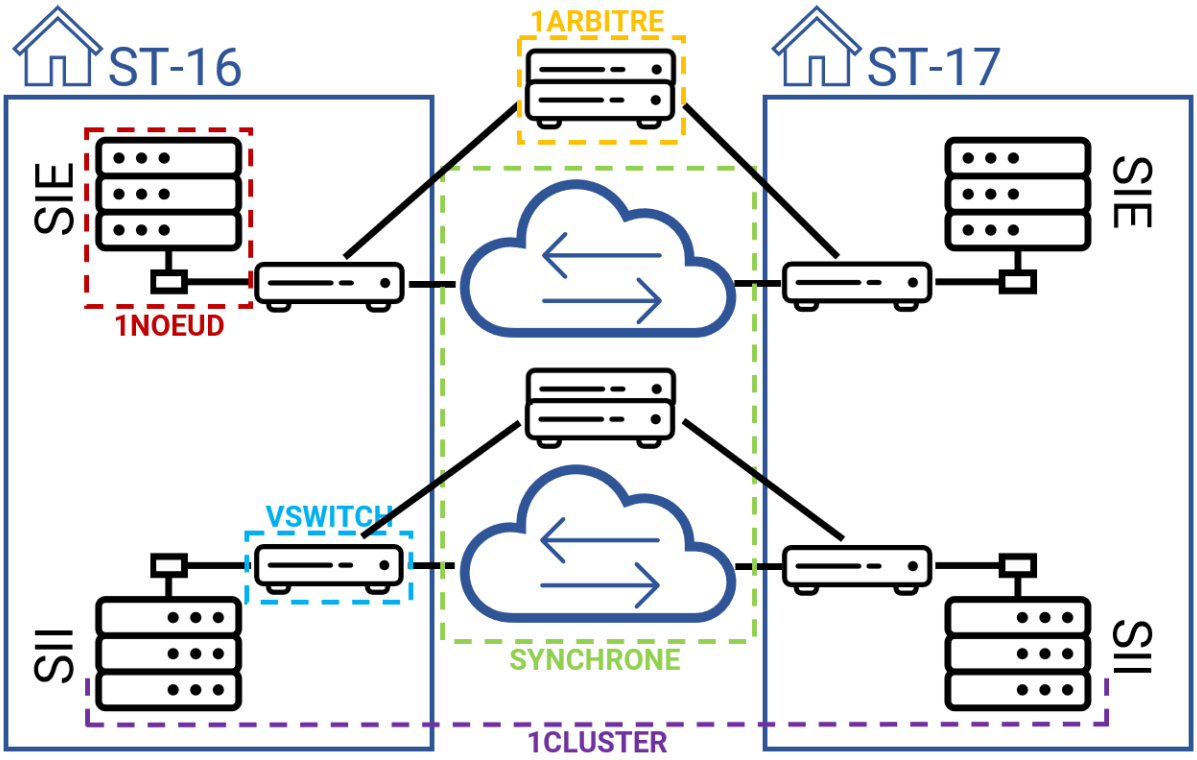


Figure 16 - Architecture Antemeta

En effet, cette solution, grâce à cet arbitre n'est pas soumise aux problèmes de « Split-Brain » que nous allons détailler immédiatement.

2.4.5.4\ Split-Brain

Dans les systèmes d'information redondés, il existe un scénario catastrophique appelé le « Split-Brain ». Il peut se traduire par « Cerveaux divisés » en français, il s'agit d'un incident où le système d'information possède plusieurs maîtres sur les mêmes données de stockage.

Prenons par exemple l'architecture proposée par TGITS et imaginons une panne à l'endroit marqué par un cercle rouge barré (par simplicité, je n'ai récupéré que le système d'information SIE) :

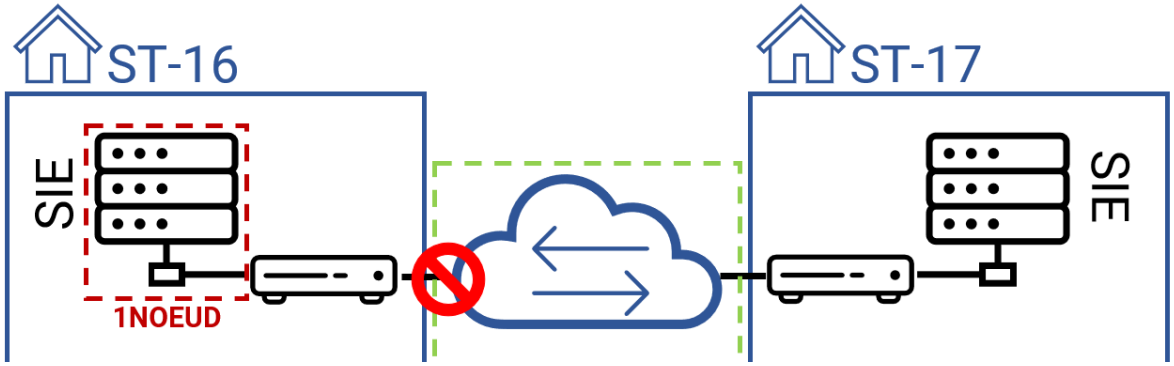


Figure 17 - Exemple de panne sur l'infrastructure TGITS

Dans cette panne, aucun des nœuds n'est tombé, cependant, ils ont tous les deux détecté l'indisponibilité de l'autre nœud. En effet, la panne est arrivée au niveau du lien entre les deux équipements.

Par conséquent, les deux nœuds vont recevoir une alerte disant que l'autre nœud est tombé. Dans ce genre de cas, le comportement normal de chacun des nœuds va être de démarrer toutes les VM qui étaient sous la responsabilité du nœud distant.

En conclusion, chaque VM sera virtualisée à deux endroits différents, générant des conflits sur le réseau. De plus, si cet incident n'est pas vite identifié, les données des VM vont être changées, car elles sont toujours exploitées par d'autres services et il sera impossible de fusionner ces données, la solution sera alors de tuer une des deux VM, ayant pour conséquence la perte de certaines données.

Aussi, supposons que la panne soit levée ayant la résolution du Split-Brain, chaque nœud verra chaque VM doublée et des comportements étranges et imprévisibles commenceront à émerger, par exemple, l'arrêt des VM, ou des tentatives de synchronisation avec des données différentes.

Maintenant, prenons la même panne sur l'architecture d'Antemeta :

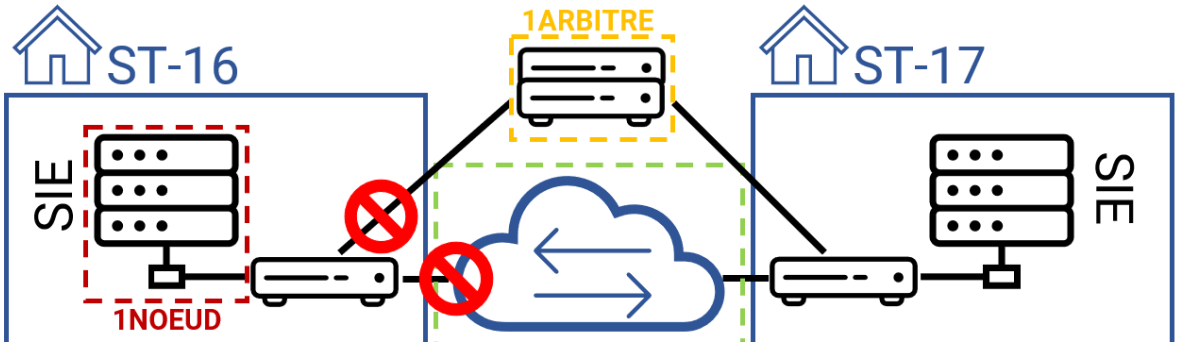


Figure 18 – Exemple de panne sur l'infrastructure Antemeta

Avec cette topologie, la démocratie prime, le nœud dans la salle ST-16 va voir qu'il est fonctionnel, mais seul, il va alors arrêter toutes les VM et se mettre en état de panne. De l'autre côté, le nœud à ST-17 va constater la perte du nœud distant puis que l'arbitre est toujours joignable ; quant à ce dernier, il va constater l'indisponibilité du nœud à ST-16 et va alors confirmer que le nœud à ST-17 doit démarrer les VM ayant été perdues.

Si la panne réseau est corrigée, le nœud de ST-16 est de nouveau disponible avec aucune VM, il va alors faire une requête à l'autre nœud pour lui proposer de répartir la charge et d'ainsi récupérer des VM ainsi que les données qui ont été modifiées lors de sa panne.

En conclusion, cette architecture est beaucoup plus sûre pour la cohérence des données, peu importe où a lieu la panne réseau, avant de faire une action, les nœuds vont toujours vérifier qu'ils sont en supériorité de vote sur le réseau.

Mais cette architecture soulève de nouveaux couts pour TotalEnergies, en effet, l'arbitre doit être placé dans une troisième salle technique, ce qui engendre de nouveaux couts, notamment sur le passage de fibres optiques jusqu'à une troisième salle.

Si nous mettons l'arbitre dans la même salle qu'un nœud, nous rajoutons un nouveau risque de scénario catastrophique. En effet, si cette salle venait à être détruite, l'arbitre ainsi qu'un nœud ne seraient plus disponibles.

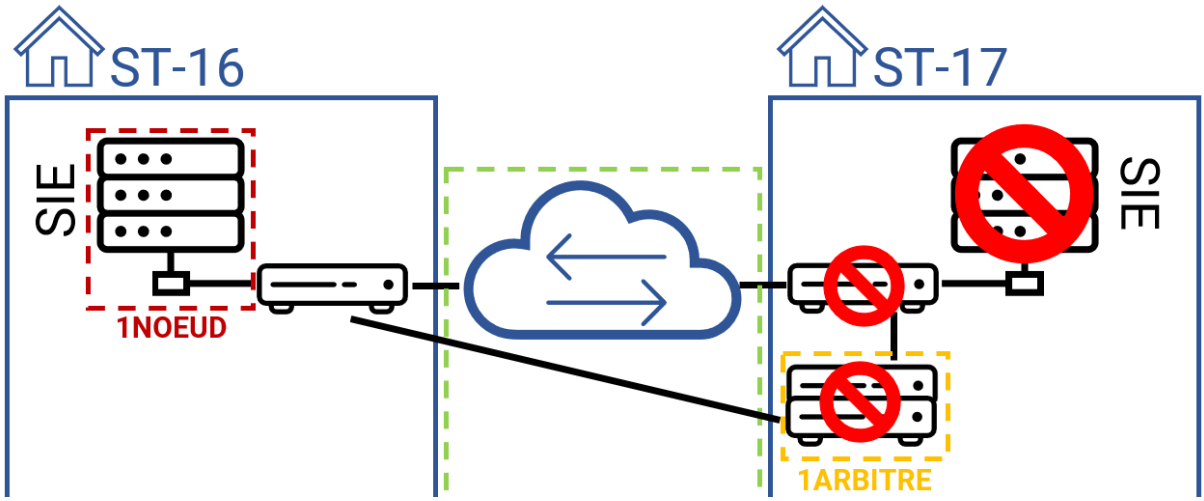


Figure 19 - Exemple lors d'une destruction d'une salle technique

En résultante, le dernier nœud, dans notre exemple à ST-16, va constater qu'il ne peut ni joindre l'arbitre ni joindre le nœud distant, il va donc se détecter comme seul et initier la même procédure que précédemment, c'est-à-dire l'arrêt des VM et la mise en état de panne du nœud.

Ainsi, nous nous retrouvons avec un système d'information complètement indisponible alors qu'un nœud pourrait toujours assurer la disponibilité des données, nous perdons alors notre redondance.

2.4.5.5\ Architecture retenue

Comme vu précédemment, les offres de Antemeta et de TGITS possèdent chacun des avantages et inconvénients ; il ne s'agit pas de simples différences de taille de stockage ou de puissance de calcul.

Afin de trancher, j'ai effectué une « Procurement Table », il s'agit d'un tableau permettant, grâce à différents poids, de faire un choix : chaque offre possède un score de 0 à 10 dans un critère de sélection, ce score est ensuite multiplié par le poids. L'offre avec le plus grand total est la plus avantageuse pour l'entreprise.

Tableau II - Tableau comparatif des offres

Critères de sélection	TGITS	Antemeta	Poids	Score TGITS	Score Antemeta
Coût :	8	5	100%	8	5
Légalité :	10	10	100%	10	10
Facilité de transition :	7	6	40%	2.8	2.4
Sécurité :	10	10	100%	10	10
Tolérance aux pannes :	7	10	90%	6.3	9
Vitesse d'installation :	7	0	60%	4.2	0
Facilité d'utilisation :	3	3	60%	1.8	1.8
Dimensionnement :	8	9	80%	6.4	7.2
Coûts de maintenance :	8	7	80%	6.4	5.6
Scalabilité :	10	10	75%	7.5	7.5
Consommation :	8	5	20%	1.6	1
Retour d'expérience :	6	0	10%	0.6	0
			TOTAL :	65.6	59.5

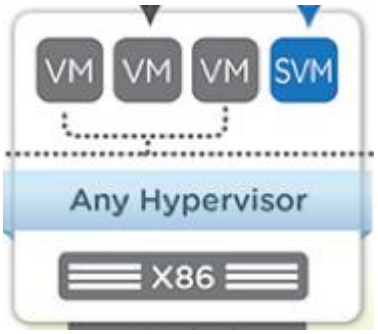
Ainsi, comme nous pouvons le constater, l'offre de TGITS est plus avantageuse et sera donc choisie, en effet, l'installation d'un arbitre demandait tellement de travaux du fait de la 3e salle technique nécessaire qu'il en a résulté en un zéro dans le critère de vitesse d'installation.

2.5\ Détail technique de la solution

2.5.1\ Fonctionnement

Pour rappel, nous avons choisi l'offre de TGITS, à savoir l'architecture Nutanix asynchrone, dans ce chapitre, nous allons détailler de manière précise le fonctionnement de cette dernière.

L'offre de TGITS consiste en, pour chaque système d'information, un cluster de deux nœuds, chaque nœud étant composé de trois serveurs. Afin de faciliter la compréhension, je vais détailler seulement le système d'information SIE sachant qu'il s'agit de la même chose pour le SII.



Ci-contre, nous avons les trois serveurs qui composent un nœud. Chaque serveur d'un nœud possède son propre hyperviseur, son propre espace de stockage ainsi que sa propre « Service Virtual Machine » (SVM). La SVM est en réalité simplement une VM dédiée pour le management de l'hyperviseur.

Figure 20 - Un serveur de l'infrastructure Nutanix

Lorsque je souhaite virtualiser des VMs, je me connecte alors à la SVM et je crée simplement une VM. Cette dernière va alors prendre des ressources de calcul ainsi que du stockage du serveur qui lui seront dédiés et elle sera alors hébergée par ce même serveur.

Maintenant, étendons la topologie à un nœud entier :

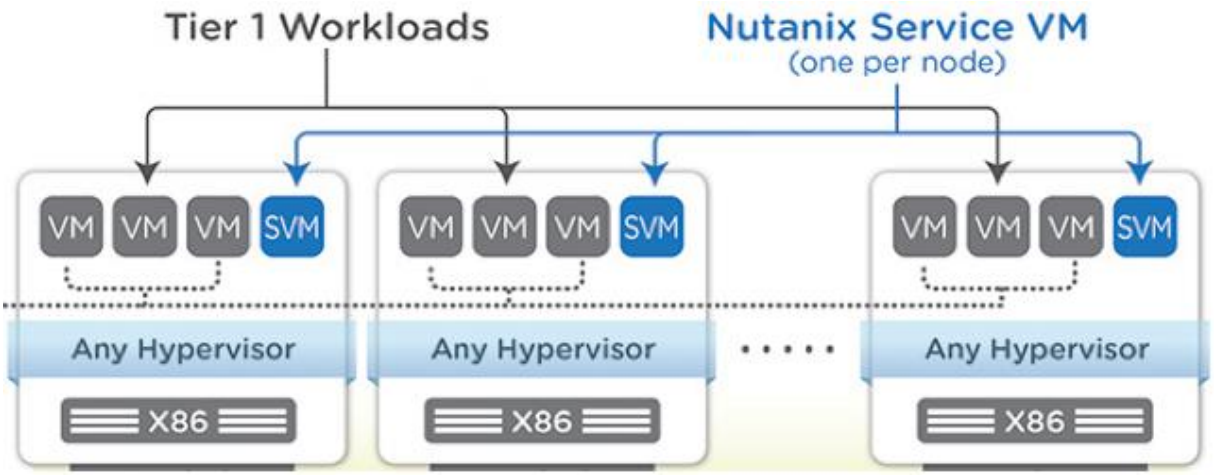


Figure 21 - Nœud de 3 serveurs Nutanix

Comme dit précédemment, chaque serveur, bien qu'il soit dans le même nœud, possède sa propre SVM, c'est-à-dire que si je souhaite créer une VM, j'ai le choix de me connecter à l'une des trois SVM.

Il s'agit là déjà d'un premier niveau de redondance, s'il n'avait qu'une seule SVM et que cette dernière venait à tomber en panne, il n'aurait pu été possible de gérer le système d'information.

La SVM possède les droits de contrôle sur son hyperviseur, mais aussi sur celui des autres, il est tout à fait possible de se connecter à la SVM du second serveur pour créer une VM sur le premier ou troisième serveur. Cela signifie qu'en cas de panne d'une SVM, une des deux restantes pourra toujours contrôler l'hyperviseur local.

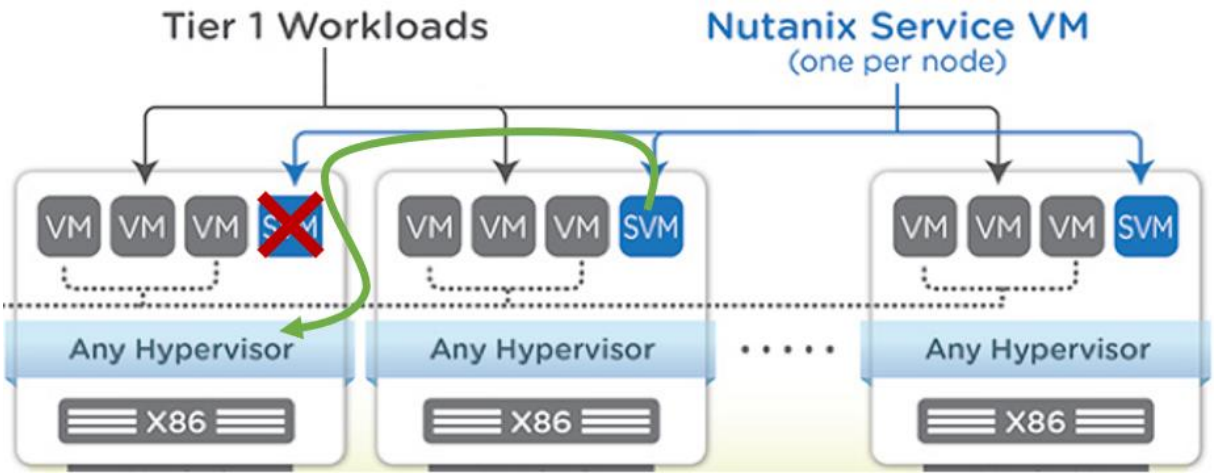


Figure 22 - Exemple de panne de SVM

Ainsi, le système est tolérant à la panne de deux SVM, en effet, bien que nous soyons dans une architecture d'un cluster de deux nœuds, les SVM possèdent le contrôle de l'hyperviseur seulement sur leur propre nœud et non sur celui distant.

2.5.2\ Redondance à facteur trois

Pour notre système d'information, nous avons fixé le facteur de redondance à 3, cela signifie que pour chaque VM, il existe 3 emplacements de stockage différents, assurant ainsi un certain degré de redondance. Dans notre cas, en plus de la VM originale, deux copies sont créées, une localement et une sur le nœud distant.

Prenons un exemple où est créée une VM de couleur verte sur le serveur 1 du nœud 1, la SVM de ce dernier va en parallèle copier la VM dans un autre nœud du même nœud sans la démarrer. Cette copie est complètement cohérente avec la VM originale, il n'y a pas de delta de différence dans les données.

Ensuite, tous les « X » temps, supposons une heure pour notre exemple, les nœuds s'envoient des copies de leurs VM afin d'assurer une redondance géographique, cependant, ces sauvegardes possèdent un delta de différence, ici d'une heure, et sont donc incohérences et utilisées seulement dans le cas où les deux précédents espaces de stockage sont perdus.

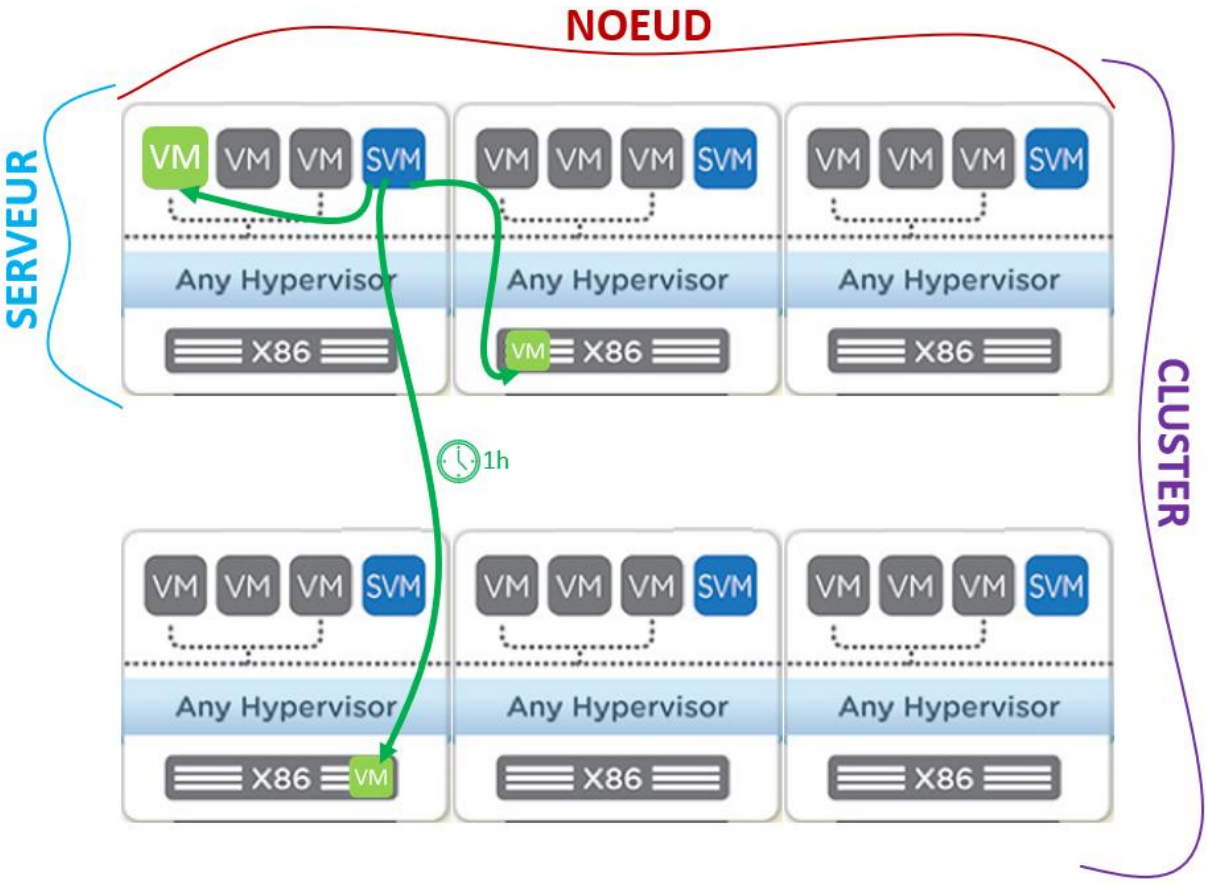


Figure 23 - Réplication à facteur 3

Avec cette architecture, nous pouvons faire face à plusieurs pannes tant la redondance est assurée.

Supposons que le serveur 1 du nœud 1 tombe en panne, la SVM du serveur 2 va immédiatement démarrer la VM de sauvegarde et en devenir la responsable, de plus, le facteur de redondance étant tombé à 2, une copie locale sera de nouveau créée pour assurer le facteur à 3.

Pour les utilisateurs, ce genre de coupure est quasiment invisible, ils devraient simplement ressentir une petite latence le temps du démarrage de la VM.

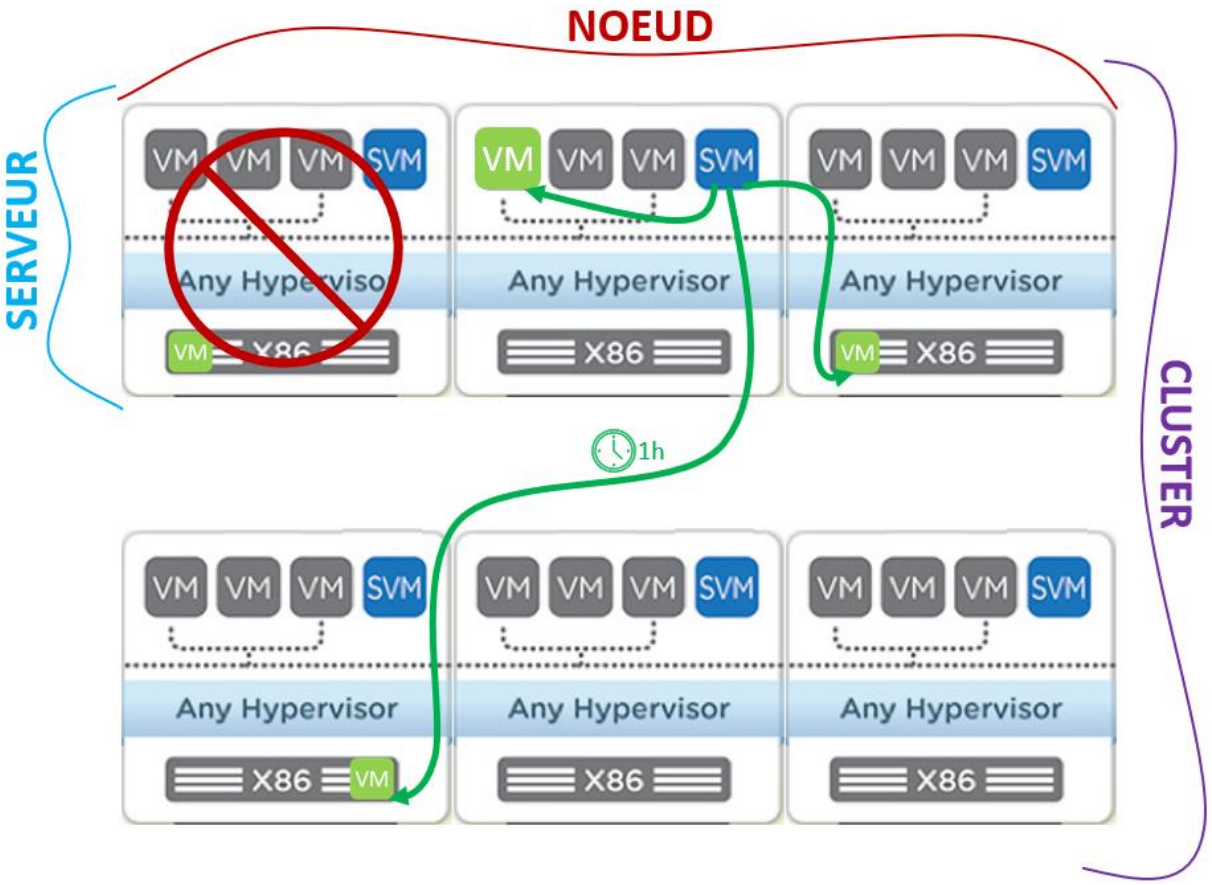


Figure 24 - Un serveur du premier nœud n'est plus fonctionnel.

Supposons que le serveur 2 tombe aussi en panne, le serveur 3 prendrait le relai, cependant, étant le dernier serveur de son nœud, il ne pourra pas faire de copie locale, le facteur de redondance sera bloqué à 2 et il s'agit d'une situation à corriger rapidement.

Enfin, si tous les serveurs du premier nœud sont de nouveau fonctionnels, le facteur de redondance sera à 4, car nous aurons 3 copies locales et une distante. La SVM en charge de la VM supprimera alors la copie locale la plus ancienne du nœud.

Dans un chapitre précédent qui présentait la solution de manière survolée, j'avais précisé que lors de l'indisponibilité d'un nœud complet, une alerte était envoyée au nœud distant pour démarrer les VM perdues. Cependant, comme aussi précisé précédemment, ce genre de comportement dans un système d'information à nœuds pairs pouvait nous entraîner dans un scénario split-brain.

Afin d'éviter ce scénario catastrophique, nous avons configuré le cluster pour qu'il ne fasse strictement rien lors de la perte d'un nœud.

Dans ce scénario, la VM verte n'est plus disponible, car elle était hébergée sur le nœud 1, bien qu'il y ait une sauvegarde sur le nœud 2, ce dernier ne la démarrera pas tant qu'il n'aura pas reçu un ordre de démarrage déclenché par une autorité humaine.

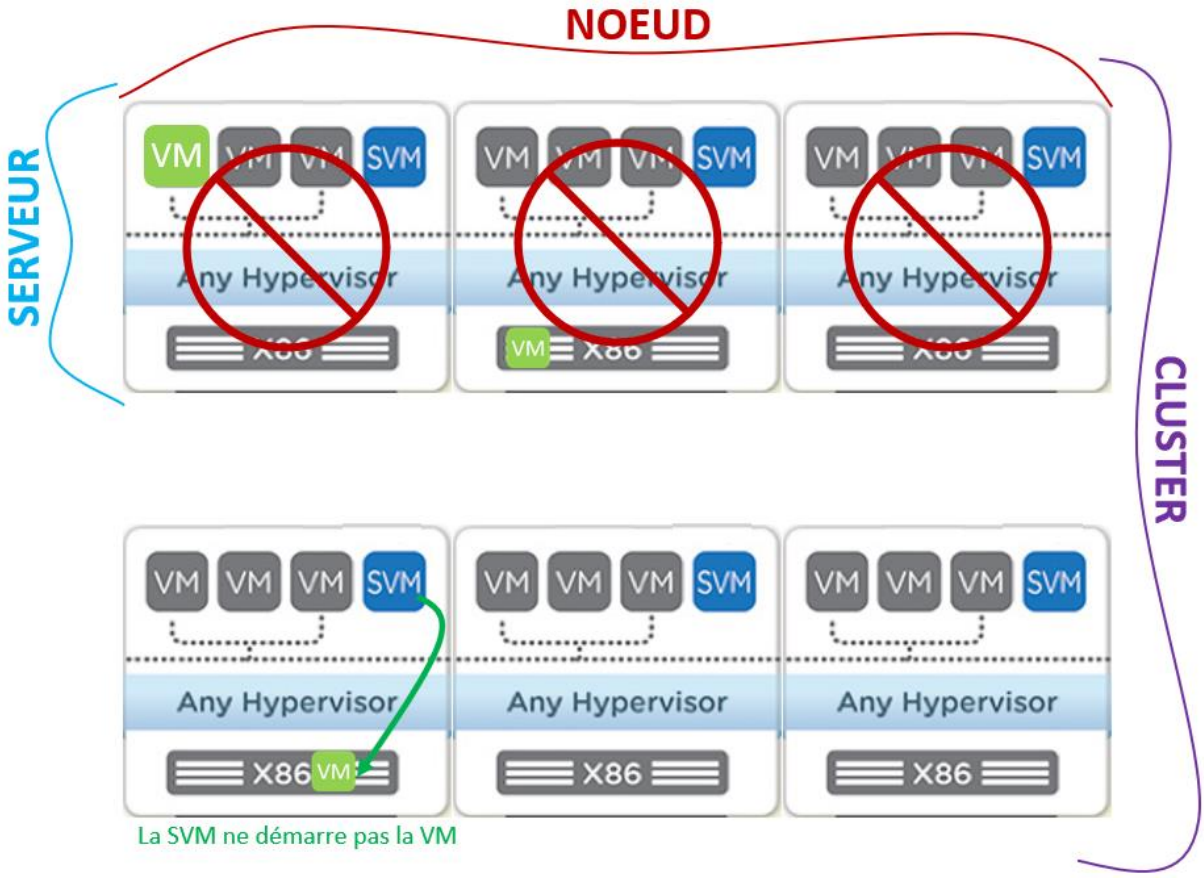


Figure 25 - Panne d'un nœud complet

Cette solution permet d'éviter les scénarios split-brain vus précédemment comme lorsque la panne est d'origine réseau et située entre les nœuds. Cette manière de fonctionnement supprime cependant au système d'information une partie de son autonomie et augmente les temps d'indisponibilité des VM en cas de panne complète d'un nœud. C'est une solution préférable plutôt que d'accepter un risque de split-brain.

2.6\ Réseautique

Dans les chapitres précédents, nous avons étudié en détail le fonctionnement de la solution proposée par TGITS. Si nous implémentons cette solution aujourd'hui, nous aurions simplement nos deux clusters SIE et SII dans deux salles géographiquement distantes ; il faut maintenant se pencher sur la question de la réseautique afin d'assurer le bon fonctionnement de nos systèmes d'information.

Dans cette partie seront détaillés tous les processus par lesquels nous sommes passés dans le but de connecter la solution Nutanix au réseau de TotalEnergies de manière à assurer la sécurité, la redondance et la disponibilité de manière optimale.

Il s'agit de l'étape du projet sur laquelle j'ai majoritairement travaillé, en effet, bien que mon poste d'administrateur réseaux et systèmes me permette de travailler dans ces deux domaines, je travaille principalement sur des projets réseau et mes connaissances sont plus approfondies dans ce domaine.

J'ai donc pu, avec l'aide de l'ingénieur réseau du projet, me pencher sur les différentes problématiques que soulevait l'architecture Nutanix pour son implémentation dans nos réseaux.

Ainsi, dans ce présent chapitre, nous aborderons des sujets tels que :

→ Le raccordement physique de la solution
→ La gestion de la commutation, c'est-à-dire le niveau 2
→ La gestion du routage, c'est-à-dire le niveau 3
→ La redondance du réseau

Bien que cette étape soit présentée après le détail de la solution de Nutanix pour faciliter la compréhension du sujet, elle s'est en réalité déroulée avant l'installation de la solution physiquement dans nos locaux, plus précisément pendant la période de livraison de cette dernière.

2.6.1\ Fibrage

Dans un premier temps, il faut penser au raccordement des nœuds entre eux pour former le cluster ; en effet, pour rappel, chaque nœud sera dans une salle technique géographiquement distante.

Cette distance implique alors des passages de fibres optiques sous les routes afin de pouvoir relier les deux points.

Le schéma suivant ne représente pas la raffinerie de Grandpuits, il sert juste de support d'illustration :

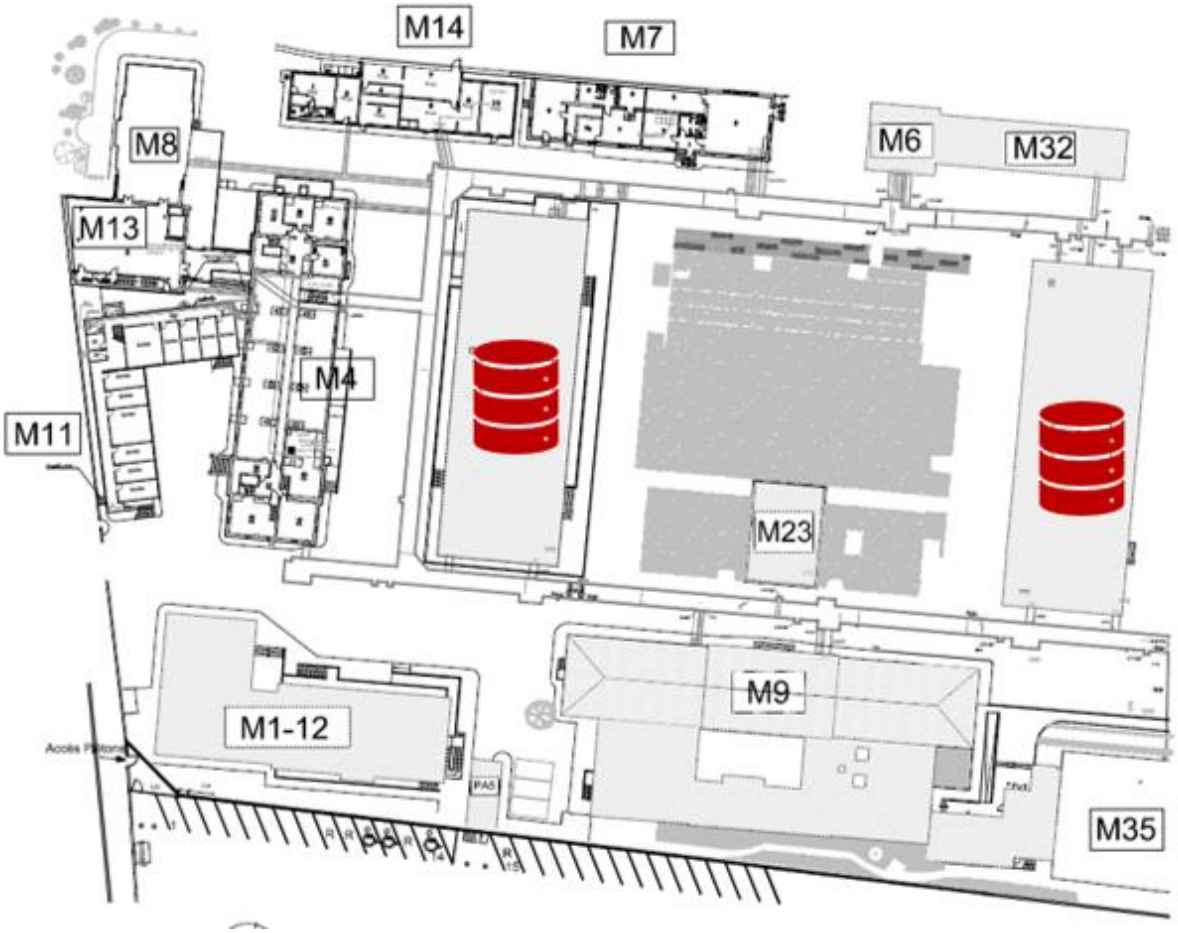


Figure 26 - Emplacement géographique de 2 nœuds

Nous pourrions raccorder les nœuds en fibres optiques par nos fibres déjà présentes sur le site, cependant, étant donné l'importance de cette architecture, il a été préféré de créer de nouveaux chemins de fibre optique dédiés.

Dans un souci de redondance, nous avons décidé d'utiliser 2 chemins de fibre optique différents, ainsi, si l'un des chemins venait à être coupé par exemple par un effondrement du bitume, un autre chemin serait toujours disponible pour le fonctionnement de l'architecture.

Pour les 2 clusters, à savoir SIE et SII, nous utiliserons les mêmes chemins de fibres, cela ne pose pas de problèmes.

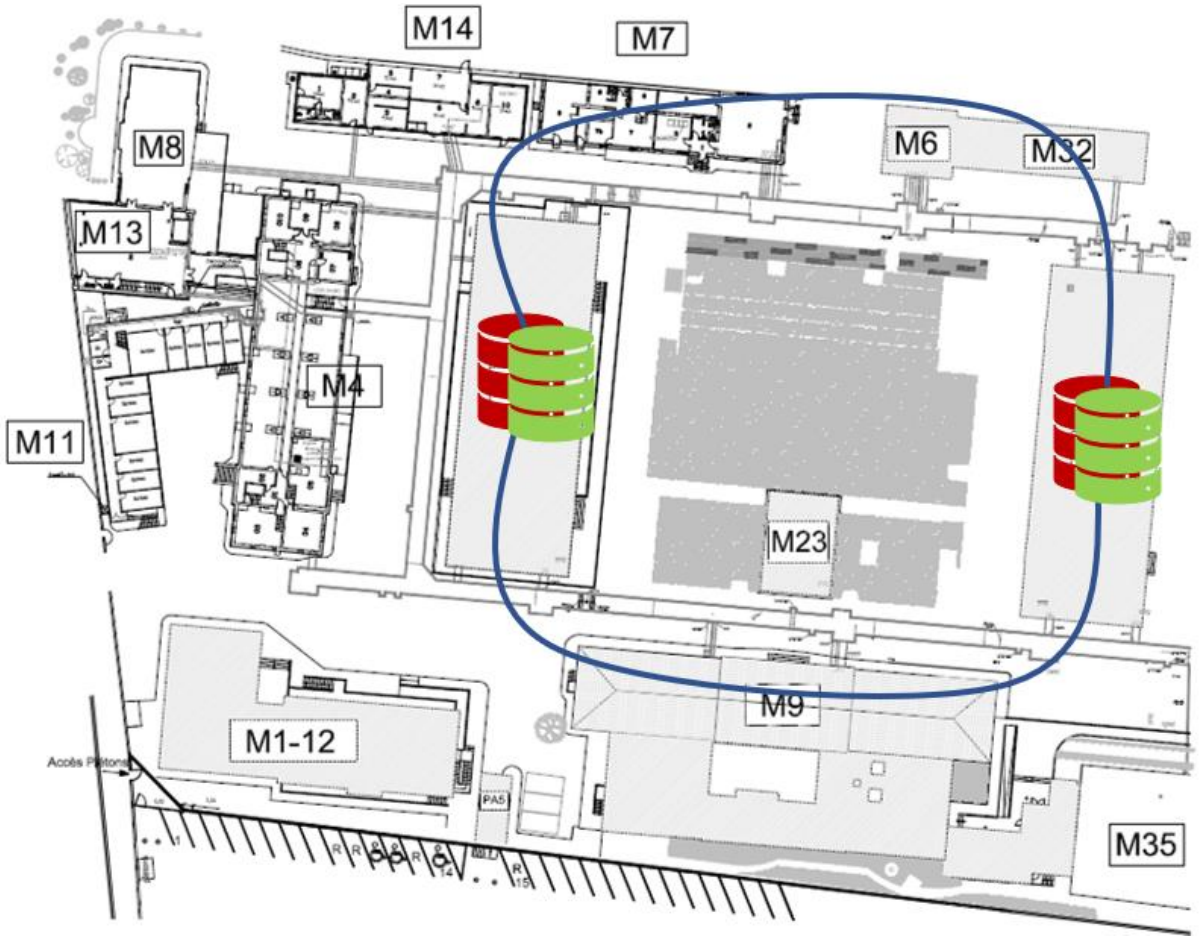


Figure 27 - Chemins des fibres optiques

La dernière question à laquelle nous devons répondre concerne le type de fibre que nous allons utiliser, à savoir de la fibre monomode ou multimode. En effet, ces deux fibres optiques possèdent des avantages et des inconvénients qu'il faut prendre en compte afin de déterminer le bon choix.

La fibre optique est une méthode de transmission de données reposant sur la lumière ; à l'intérieur des câbles de fibre optique se trouve un noyau dans lequel on envoie de la lumière, cette dernière rebondit alors dans le noyau jusqu'à la destination.

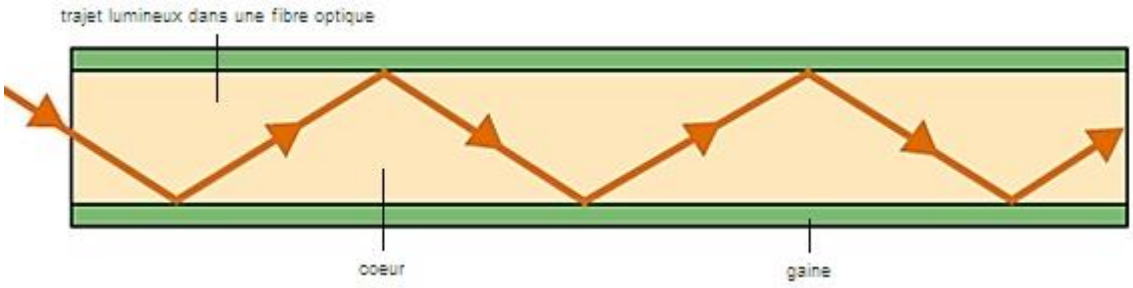


Figure 28 - Fonctionnement d'une fibre optique (Schéma de Média LAROUSSE)

Une fibre optique monomode possède un noyau beaucoup plus petit que la multimode, 9 micromètres contre 50 micromètres. Le cœur étant plus petit, la lumière effectue moins de rebonds lors de son trajet, et donc, perd moins d'intensité. De plus, du fait que la lumière effectue moins de rebonds, elle possède une trajectoire plus droite et peut donc alors permettre une vitesse de transmission supérieure.

En conclusion, que ça soit pour couvrir de grandes distances ainsi que d'assurer un débit de données maximal, la fibre monomode est en tous points supérieure à la fibre multimode. Cependant, la fibre monomode est deux à trois fois plus couteuse que la fibre multimode, de plus, afin de traduire la lumière en données, il faut utiliser des « Small Form-factor Pluggable » (SFP) qui ne peuvent être compatibles qu'avec un seul type de fibre. Ces derniers sont aussi plus couteux en version monomode.

Étant donné que l'architecture aura à charge les systèmes d'information SIE et SII qui représentent la majorité du trafic réseau de la plateforme, nous avons décidé de ne pas faire de concessions sur les prix des fibres optiques. Ainsi, nous avons donc opté pour la fibre monomode assurant un meilleur débit.

2.6.2\ Configuration du réseau

2.6.3\ Commutation

2.6.3.1\ Physique

Dans le chapitre précédent, nous avons défini notre besoin en fibre, maintenant, nous devons nous intéresser aux équipements qui nous permettront de connecter les nœuds au reste du réseau.

Afin de permettre aux serveurs Nutanix d'envoyer du trafic sur leur réseau respectif, nous devons les raccorder aux routeurs cœur de réseau. Ces derniers ont la charge du routage de leur réseau, c'est-à-dire qu'à chaque fois que du trafic réseau doit changer de VLAN, ce dernier passe forcément par le cœur de réseau pour être routé sur le réseau de destination.

Le cœur de réseau SIE est composé de 2 routeurs physiques qui n'en forment qu'un seul virtuellement, ces deux routeurs sont dans les mêmes salles techniques que notre solution Nutanix, c'est-à-dire les salles ST-16 et ST-17. Il s'agit de la même architecture pour le réseau SII, mais il s'agit de routeurs moins récents étant limités à un débit de 1Gb/s, comparé à ceux du SIE qui sont quant à eux à 10Gb/s.

Afin de raccorder les nœuds aux routeurs, nous allons utiliser des commutateurs, plus précisément, des stacks de commutateurs. En effet, si nous raccordons un nœud sur un seul commutateur, dans le cas où ce dernier tombe en panne, il en résulterait une panne d'un nœud complet, car il n'y aura plus aucun chemin possible vers ce nœud.

Afin de pallier à ce problème, chaque serveur d'un nœud sera raccordé à deux commutateurs physiques n'en formant en réalité qu'un seul virtuel, de ce fait, en cas de panne d'un des deux commutateurs, le second sera toujours disponible pour diriger le trafic des nœuds vers leur cœur de réseau respectif.

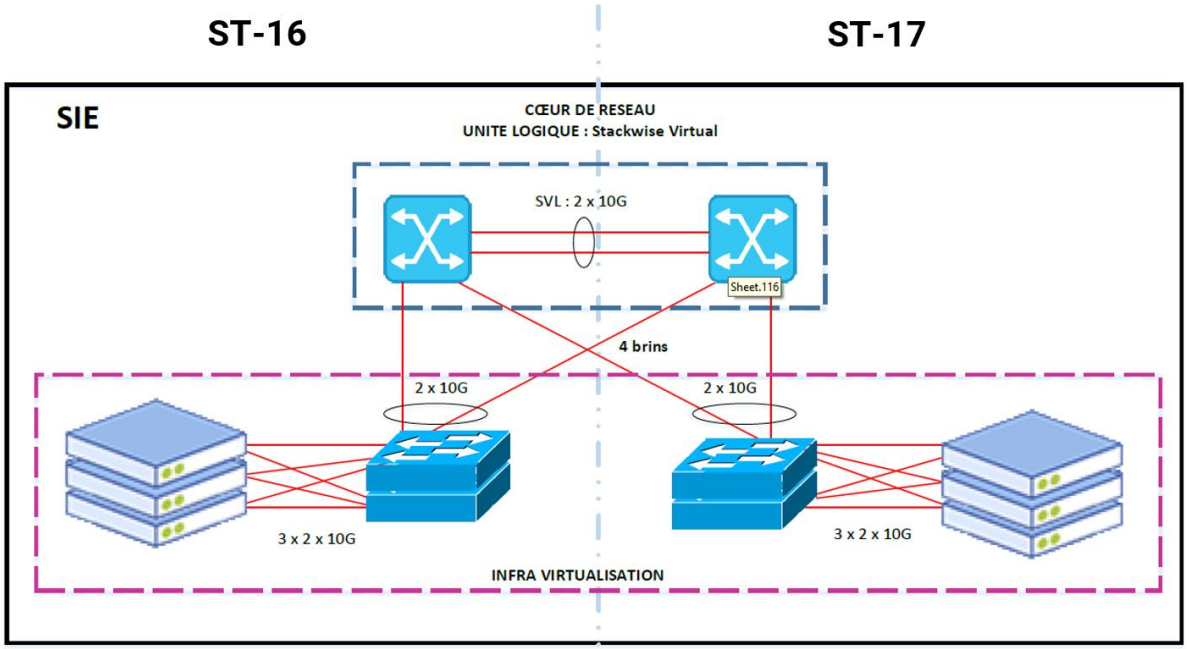


Figure 29 - Schéma réseau SIE

De plus, chaque stack de commutateur sera raccordé aux deux équipements formant le cœur de réseau pour assurer la redondance. En effet, si nous raccordons chaque stack de commutateur au cœur de réseau physique de sa salle technique, si l'un des deux équipements composant le cœur de réseau tombe en panne, il en résulterait aussi de la perte d'un nœud Nutanix complet.

En utilisant les chemins de fibres précisés dans le chapitre précédent, nous pouvons alors raccorder chaque stack de commutateur au cœur de réseau distant assurant alors une redondance renforcée.

Cette étape du projet n'est pas à négliger, comme nous l'avons vu précédemment, la redondance est un facteur important pour l'infrastructure Nutanix, nous avons vu que de manière locale, les nœuds avaient beaucoup d'outils mis à disposition afin d'éviter au maximum l'indisponibilité des VM. Si le réseau derrière cette architecture n'est pas pensé correctement, tous les efforts précédents faits au niveau du système seront vains, car le réseau ne serait alors pas fiable.

Avec cette architecture réseau, nous avons un certain degré de tolérance aux pannes ; en effet, nous avons la possibilité de perdre un des équipements du cœur de réseau ainsi qu'un commutateur par stack et même des liens entre les équipements.

La connectivité de ce réseau assure qu'à n'importe quel endroit de l'architecture, il existe toujours un chemin alternatif pour arriver d'un nœud Nutanix à un autre.

Nous avons dupliqué cette architecture pour le réseau SII, cependant, les cœurs de réseau étant moins récents, ils sont capables d'assurer seulement un débit à 1Gb/s.

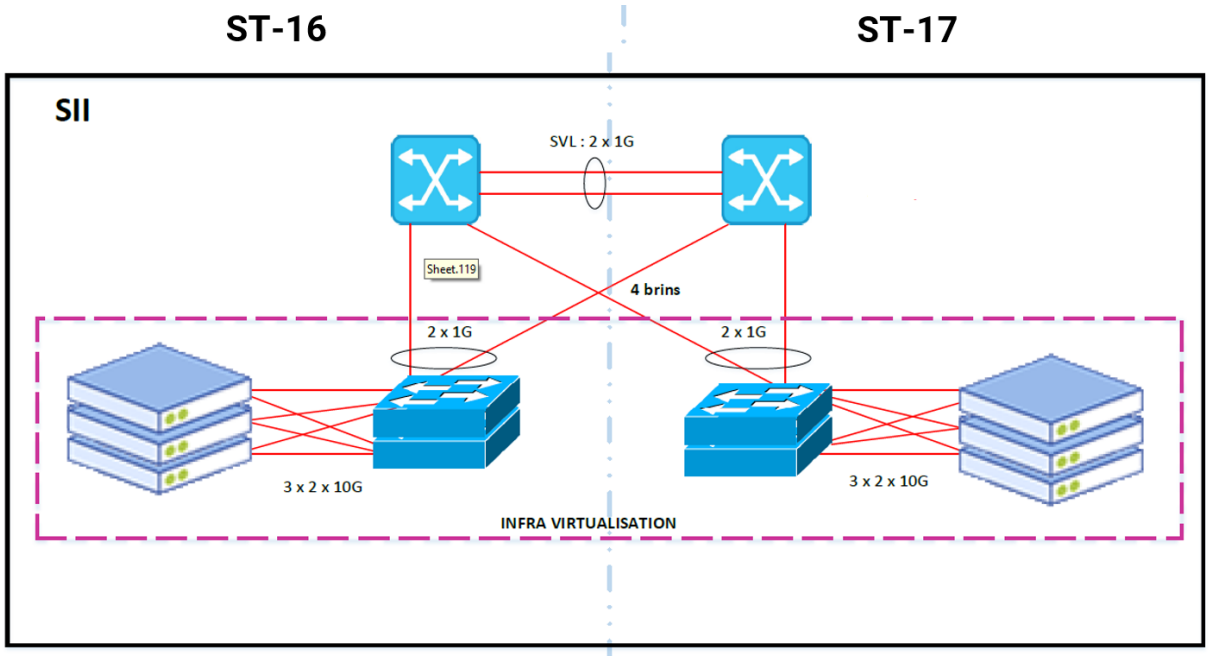


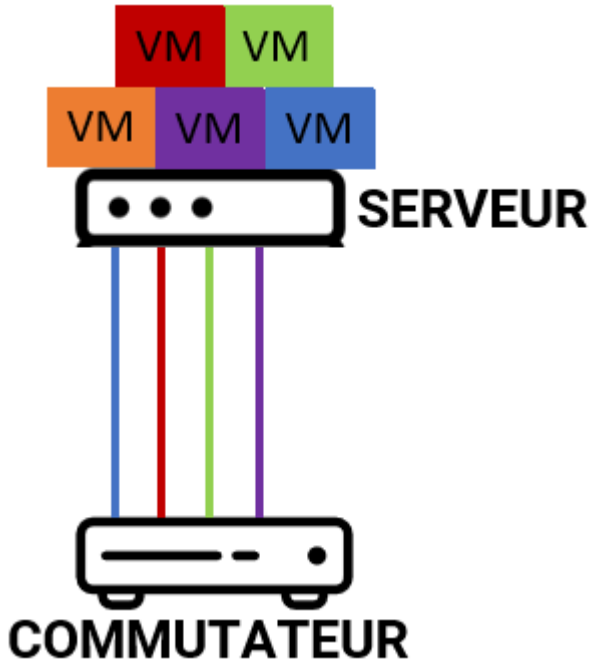
Figure 30 - Schéma réseau SII

À ce moment-là du projet, nous ne nous étions pas encore rendu compte de la problématique que soulevait ce faible débit. En effet, à la fin du projet, les liens ayant trop peu de débit étaient constamment saturés, ce qui résultait en la perte de flux de données. Nous verrons plus tard dans ce présent document comment nous pouvons pallier à ce problème.

2.6.3.2\ Virtuelle

Chaque serveur que compose un nœud Nutanix possède 4 ports Ethernet afin de raccorder les serveurs aux commutateurs. En règle générale, un port Ethernet sur un serveur correspond à une carte réseau ; si un serveur possède plusieurs cartes réseau, il peut alors être dans plusieurs réseaux à la fois en changeant l'adresse IP de chaque carte dans le système d'exploitation.

Dans notre cas, chaque serveur va virtualiser des VMs qui seront dans des VLANs différents et il y en aura bien plus que 4 différents. Ceci nous amène à une nouvelle problématique, si nous virtualisons par exemple 5 VMs dans 5 VLANs différents, un de ces derniers ne pourra pas être joignable, car le serveur ne possède que 4 cartes réseau, le rendant alors accessible seulement sur 4 réseaux différents.



Dans le schéma ci-contre, les 4 cartes réseau sont raccordées à un même commutateur, chaque carte réseau est dans un réseau différent illustré par les différentes couleurs.

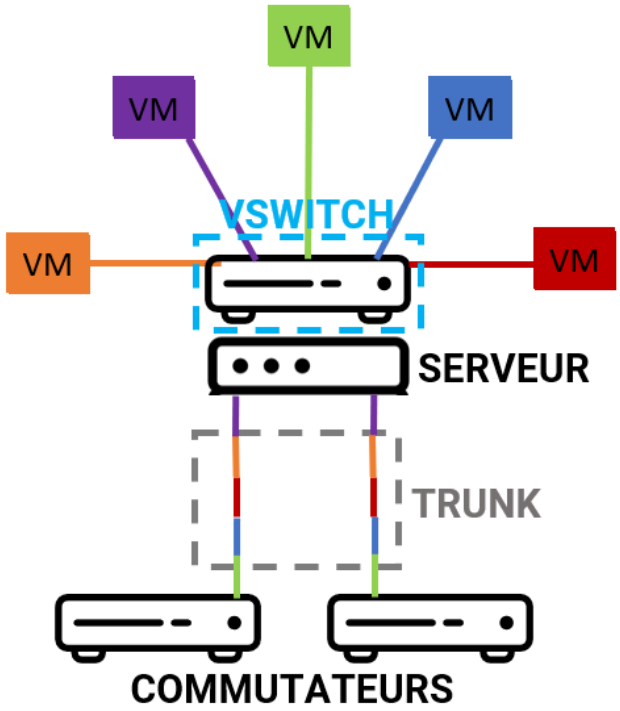
Comme nous pouvons le constater, la VM orange est dans un réseau qui n'est raccordé à aucune carte réseau du serveur. En résultante, bien qu'elle soit démarrée et fonctionnelle, la VM orange n'est pas joignable, car il n'existe aucun chemin menant à elle.

Figure 31 - Exemple d'une VM non atteignable

De plus, comme vu précédemment, nous utilisons 2 commutateurs, ce qui rend la tâche encore moins possible, vu que, dans le meilleur des cas, nous pourrions raccorder 2 cartes à un commutateur, et les 2 autres cartes à l'autre commutateur. En résultante, si un commutateur venait à ne plus fonctionner, 2 VLANs ne seraient alors plus joignables.

Pour résoudre ce problème, il faut que le nœud virtualise un commutateur, de ce fait, nous pourrons configurer les ports Ethernet de chaque serveur pour les traiter comme des ports de commutateur. Cette manipulation nous permettra alors de faire de ces ports, des ports trunk.

Un trunk (ou tronc en français) permet de faire passer du trafic de plusieurs VLANs sur un même lien, ce qui signifie qu'il sera alors possible d'accéder à toutes les VMs, quel que soit leur réseau en n'utilisant qu'un seul lien.



Dans le schéma ci-contre, le serveur virtualise un commutateur (vSwitch), de ce fait nous avons seulement besoin d'un seul port Ethernet qui est alors configuré en mode trunk permettant ainsi de faire passer le trafic de tous les VLANs différents.

Une fois le trafic arrivé au serveur, le vSwitch s'occupe de le rediriger vers les VMs concernées.

Nous pouvons alors avoir un nombre bien plus conséquent de VLANs différents.

Figure 32 - Architecture avec commutateur virtuel

Enfin, nous avons la possibilité d'utiliser seulement 2 ports Ethernet par serveur qui iront se raccorder chacun à un commutateur physique différent. De ce fait, si un des deux commutateurs venait à tomber en panne, l'autre commutateur pourra toujours assurer l'accessibilité à l'entièreté des VLANs et donc, aux VMs.

2.6.5\ Routage

Dans ce chapitre, nous allons détailler la solution de routage qui a été retenue pour notre nouvelle architecture Nutanix.

Une action de routage consiste à permettre à un paquet IP de changer de réseau, de manière générale, le routage permet simplement la connectivité des différents réseaux.

La solution Nutanix visant à virtualiser plusieurs serveurs de multiples réseaux qui auront pour but de parfois communiquer entre eux nécessite alors une solution de routage. Afin de permettre le routage du trafic informatique, un équipement de niveau 3 est nécessaire, il peut s'agir d'un routeur, d'un pare-feu ou encore d'un commutateur niveau 3.

Il existe différents types de routages, dans un premier temps, le routage statique qui consiste à renseigner toutes les routes manuellement dans le routeur. Cette solution possède de nombreux désavantages, dans un premier temps, elle demande beaucoup de configuration dans l'équipement puisqu'il faut renseigner toutes les routes possibles de chaque paquet IP en fonction de sa source et sa destination ; de plus, en cas de panne d'un lien les routes ne sont pas recalculées par le routeur ce qui n'assure pas de redondance.

Le routage dynamique quant à lui est facile d'implémentation puisque les routes ne sont pas écrites manuellement par un utilisateur ; en effet, en cas de routage dynamique, le routeur annonce aux autres routeurs à quels réseaux il est connecté puis chaque routeur calcule sa propre table de routage pour les paquets IP.

Dans notre topologie, les cœurs de réseau sont des routeurs, ce seront eux qui auront alors la tâche de router les paquets IP permettant ainsi la communication entre les différents réseaux.

Cela signifie que même dans le cas où deux VMs virtualisées par le même nœud souhaitent communiquer entre eux, le trafic remontera systématiquement jusqu'au routeur pour se faire router et ainsi changer de réseau.

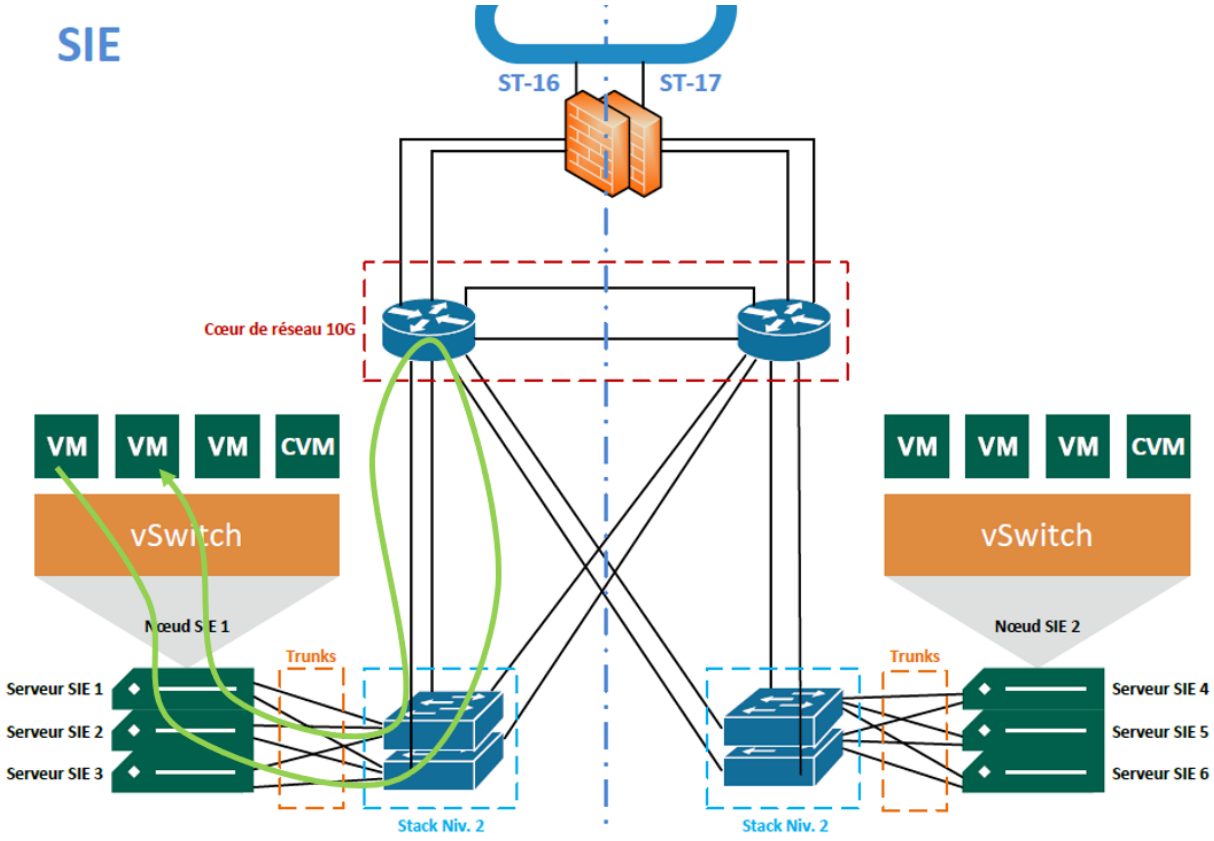


Figure 33 - Chemin du routage

Avec le schéma précédent, nous pouvons observer que le trafic devant changer de réseau doit systématiquement rencontrer un équipement de niveau 3 pour permettre son routage vers le réseau distant.

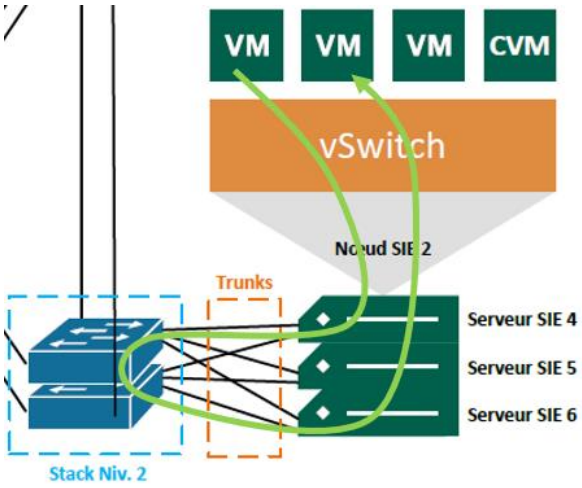


Figure 34 - Commutation réseau

Cependant, si des VM devant communiquer entre elles sont dans le même réseau, alors il n'y a pas besoin de routage .

En effet, le trafic passera seulement par les commutateurs physiques situés entre le cœur de réseau et les serveurs avant d'arriver à sa destination.

Cependant, nous pouvons observer que dans notre architecture, toutes les VMs sont dans des réseaux directement connectés aux routeurs du cœur de réseau. De ce fait, les routeurs connaissent alors directement les réseaux puisqu'il s'agit de réseaux accessibles directement par l'une de leurs interfaces.

En conclusion, nous pourrons nous passer du routage statique et dynamique, en effet, chaque VM aura comme passerelle par défaut une adresse partagée virtuelle située sur les cœurs de réseau ; de ce fait, lorsqu'une VM devra envoyer des paquets IP vers un autre réseau, elle dirigera directement son trafic vers le cœur de réseau.

Sur ce dernier, il nous suffit de créer simplement cette adresse partagée virtuelle sous la force d'une « Interface VLAN » qui sera alors la destination de tous les paquets IP ayant pour objectif d'être routés. Lors de la réception de ces paquets IP, le cœur de réseau les routera vers le réseau de destination qu'il connaitra automatiquement vu que ce dernier est connecté aux interfaces des routeurs.

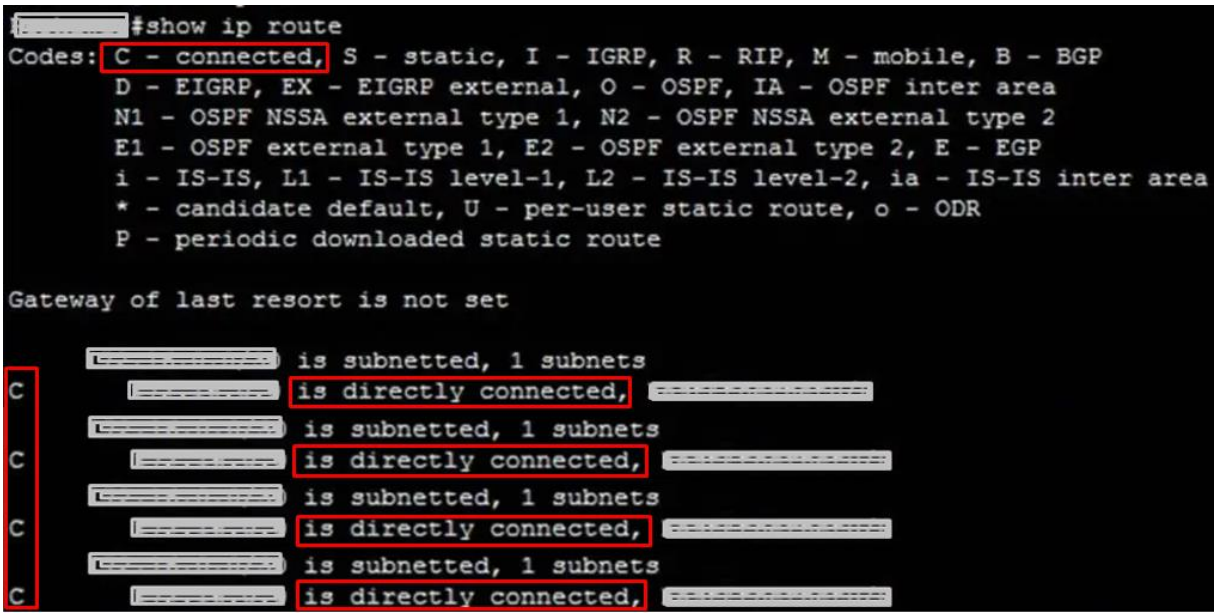


Figure 35 - Table de routage

Comme nous pouvons le constater dans la table de routage, la lettre C indique un réseau directement connecté ; or, tous les réseaux de chaque VM sont directement connectés ce qui nous permet, en conclusion, de nous passer d'un protocole de routage.

Il ne reste alors plus qu'à déclarer une seule route statique par défaut à destination du réseau SII pour les quelques paquets IP ayant pour destination ce dernier. En effet, les réseaux SIE et SII sont séparés par des pare-feux ainsi que d'autres équipements réseau, le cœur de réseau ne connait donc pas les réseaux de destination SII.

Pour ce faire, il suffit de déclarer notre route statique par défaut, ainsi, lors de trafic vers le réseau SII, le cœur de réseau envoie alors le paquet IP au cluster de pare-feux qui, lui, possède le cheminement vers ce réseau.

Tableau III - Commande de route statique par défaut

```
ip route 0.0.0.0 0.0.0.0 [Adresse IP de pare-feu]
```

Ainsi, le trafic est correctement dirigé vers le réseau SII.

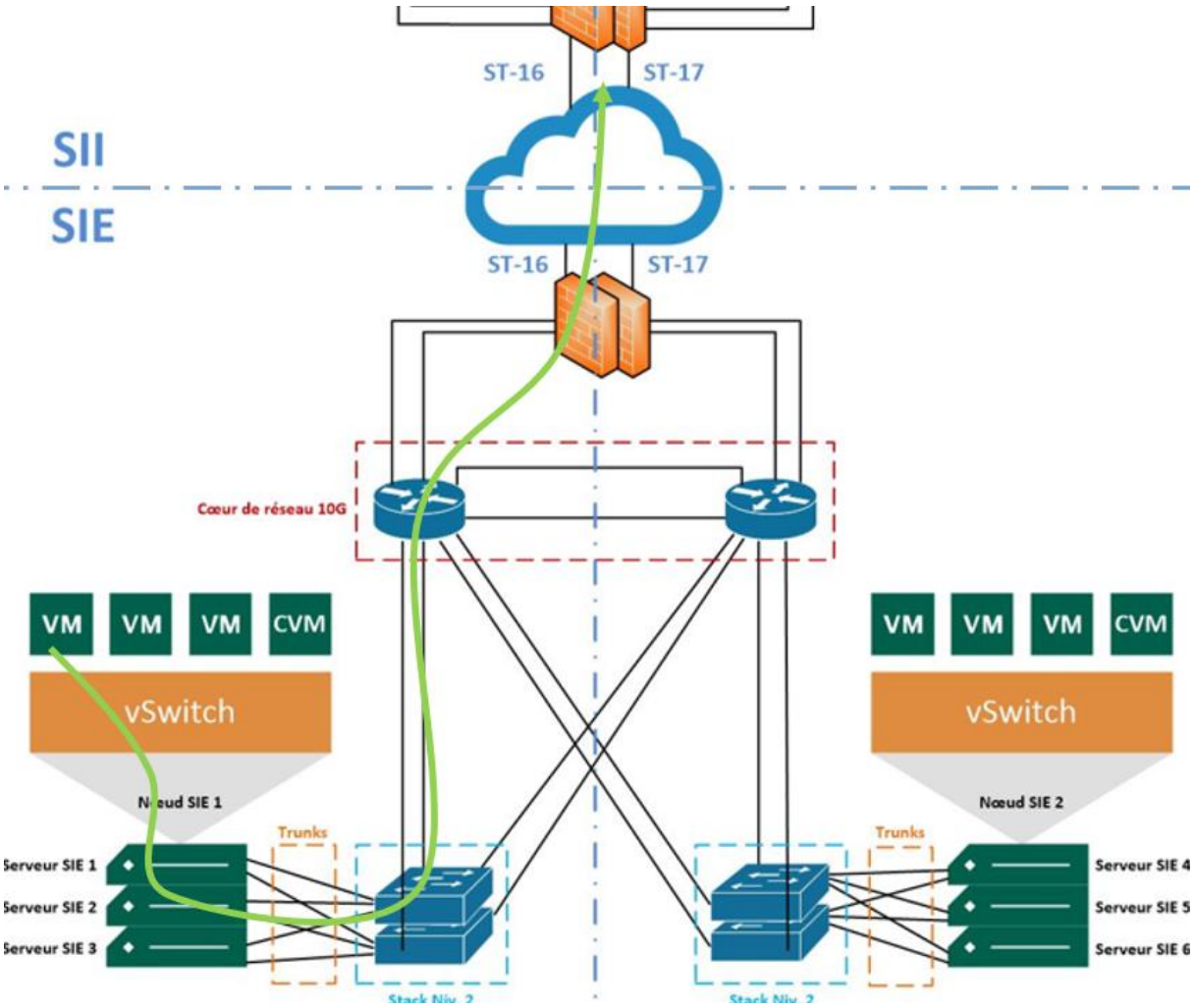


Figure 36 - Chemin d'un paquet IP à destination du réseau SII

2.6.6\ Récapitulatif

Dans cette partie, nous avons détaillé la partie réseau sur plusieurs couches du modèle « Open Systems Interconnection » (OSI), que ça soit du niveau 1 avec les différentes méthodes de connexion physiques ; le niveau 2 par la distribution du trafic IP ainsi que le niveau 3 en permettant le routage.

Toujours dans un souci de simplicité, les explications et détails techniques n'ont été donnés que sur la partie SIE du réseau, cependant, la partie SII étant une réplication de l'architecture SIE, les détails et solutions données ont été implémentés de la même manière. Le schéma complet de l'architecture est disponible en annexes (*cf. : Schéma réseau*).

A cet instant du projet, l'ensemble de l'infrastructure Nutanix peut communiquer de manière à être fonctionnelle et fiable, il est alors maintenant possible de commencer à basculer vers cette nouvelle infrastructure en commençant la partie virtualisation.

2.7\ Virtualisation

La partie réseau étant terminée à ce niveau du projet, nous avons maintenant la possibilité d'entamer la dernière étape du projet, à savoir la création des VMs.

Il existe deux cas de figure lors de la création de VM ; nous pouvons partir de zéro, c'est-à-dire créer un serveur virtualisé sans aucune donnée. Ou alors, nous pouvons créer une VM d'un serveur déjà existant physiquement, dans ce cas de figure nous souhaitons conserver les données lors du passage de physique à virtuel.

Selon le serveur à virtualiser, nous choisirons l'une ou l'autre de ces deux manières de procéder, par exemple, s'il s'agit d'un serveur hébergeant seulement quelques applications, il sera plus judicieux de créer une nouvelle VM et d'y installer les applicatifs. À l'inverse, s'il s'agit d'un serveur possédant beaucoup de données importantes ou des services Windows personnalisés, il sera alors préférable de créer une VM depuis une copie de son état physique.

La création d'une VM à partir d'un serveur physique possède plusieurs contraintes ; dans un premier temps, il est difficile de pouvoir redimensionner la VM si par exemple le serveur manquait de ressources lors de son état physique. En effet, il est parfois compliqué de rajouter des processeurs ou de la RAM virtuellement, ce problème est souvent rencontré lorsque le serveur possède une ancienne version de Windows.

De plus, cette solution demande beaucoup plus de temps que de simplement créer une nouvelle VM vide et est souvent sujette à des problèmes système ; cependant, bien qu'il y ait autant de contraintes, ce sera dans la majeure partie des cas cette méthode de virtualisation qui sera choisie afin d'éviter la perte de données de nos serveurs physiques.

2.7.1\ Nouvelle VM

Pour la création d'une nouvelle VM à partir de zéro, il suffit de nous connecter à n'importe quelle SVM de notre cluster et d'utiliser le menu de création des VMs. La SVM nous permet d'avoir un retour graphique structuré plutôt qu'un invité de commande ce qui facilite la création.

Dans un premier temps, nous renseignons les ressources qui seront utilisées par la VM :

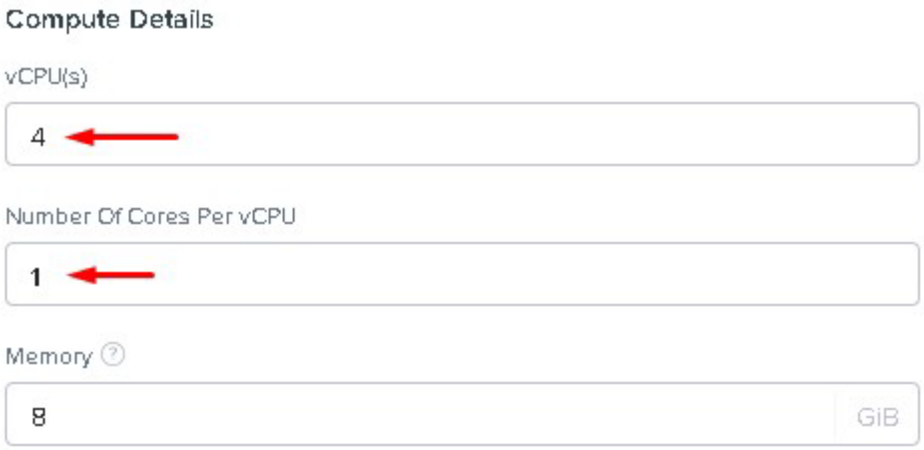


Figure 37 - Renseignement des ressources utilisées pour une VM

Dans cet exemple, la VM utilisera 8Go de RAM et 4 cœurs virtuels avec un ratio de 1 cœur physique utilisé pour 4 cœurs virtuels, il s'agit du ratio conseillé par VMware. Ensuite, nous renseignons le système d'exploitation qui sera installé en virtualisant le lecteur CD et une image :

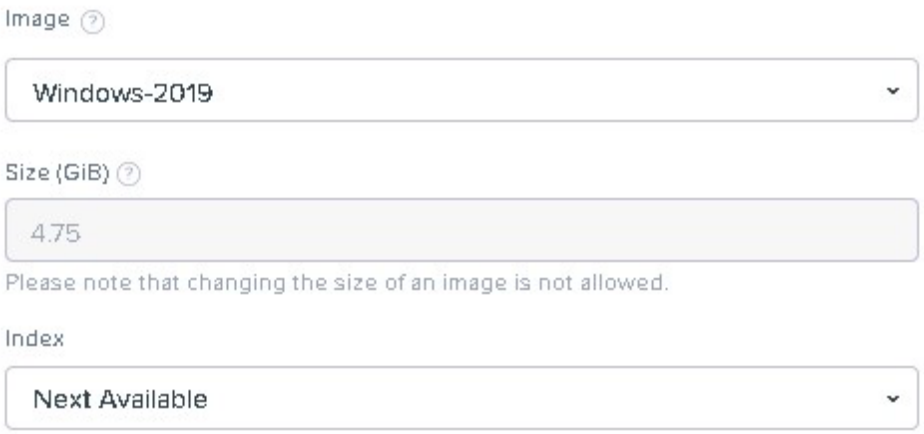


Figure 38 - Renseignement du système d'exploitation

Puis, nous allouons l'espace de stockage pour la VM :

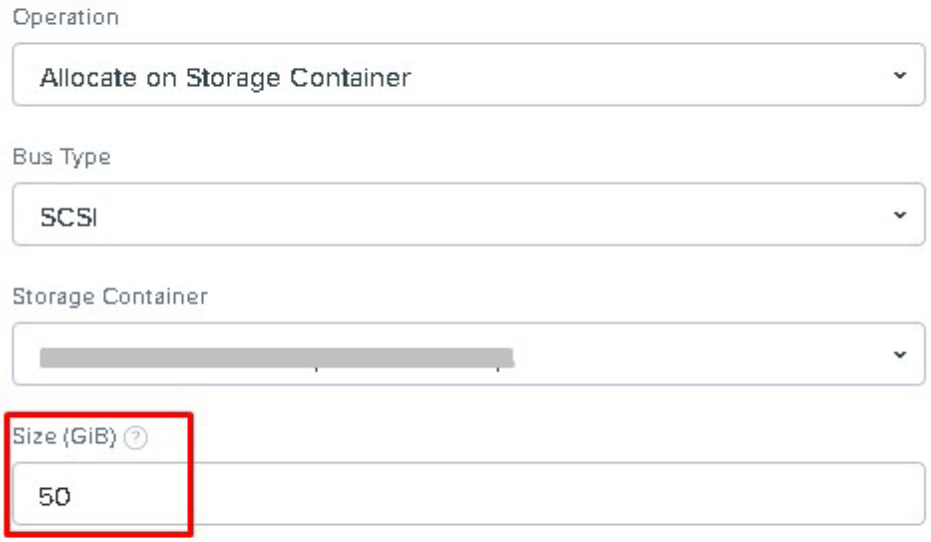


Figure 39 - Renseignement du stockage

Ici, nous allouons 50Go d'espace de stockage qui sera utilisé sur l'un des 6 serveurs composant un nœud, il est possible de choisir lequel dans le paramètre « Storage Container » ; bien évidemment, cette valeur est modifiable plus tard si nous le souhaitons.

Enfin, il ne reste plus qu'à renseigner le réseau de la VM en lui ajoutant une carte réseau virtuelle et un VLAN, c'est grâce à ces paramètres que le commutateur virtuel pourra rediriger le trafic comme vu précédemment.

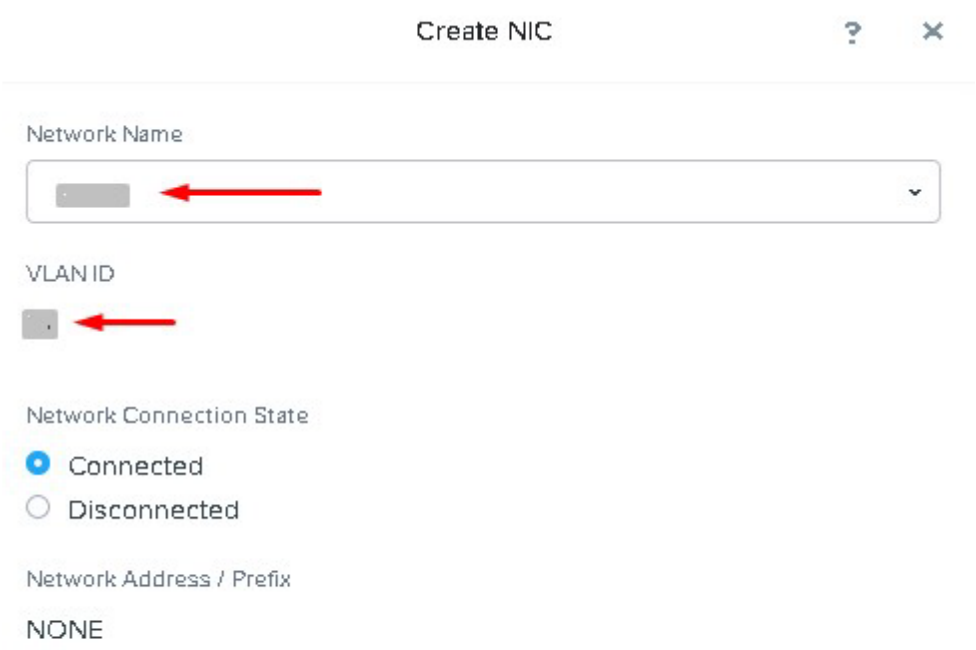


Figure 40 - Renseignement réseau

Une fois cette étape terminée, il suffit de démarrer la VM et elle sera alors disponible sur le réseau :

Figure 41 - VM fonctionnelle

Comme nous pouvons le voir, le voyant vert de la VM « Test20193 » indique qu'elle est en ligne et actuellement hébergée sur le serveur Nutanix « F############ ».

2.7.2\ Physique à virtuel

Comme dit précédemment, la méthode de virtualisation « Physical to Virtual » (P2V) sera la méthode que nous utiliserons le plus souvent du fait de son avantage de pouvoir conserver les données relatives aux serveurs dans leur état physique.

Afin d'effectuer cette action de virtualisation, nous devons dans un premier temps créer un fichier « International Organization for Standardization » (ISO) qui doit contenir les informations actuelles du serveur physique que nous allons virtualiser.

Il existe des logiciels permettant de convertir les données des serveurs en fichier ISO, malheureusement Nutanix ne possède pas son propre convertisseur, nous devons alors passer par un autre constructeur. Notre choix s'est alors porté sur « vCenter Converter », un logiciel de l'entreprise VMware, leader des solutions de virtualisation.

Afin de créer notre fichier ISO, il nous faut installer sur le serveur physique la partie « esclave » du logiciel, cette dernière, lors de la réception d'un ordre de la partie « maître » va récupérer les données du serveur à l'instant présent et créer notre fichier ISO. Afin de faciliter le P2V, nous installons la partie « maître » sur un ordinateur d'administration qui pourra alors envoyer l'ordre à tous les serveurs possédant le logiciel « esclave ».

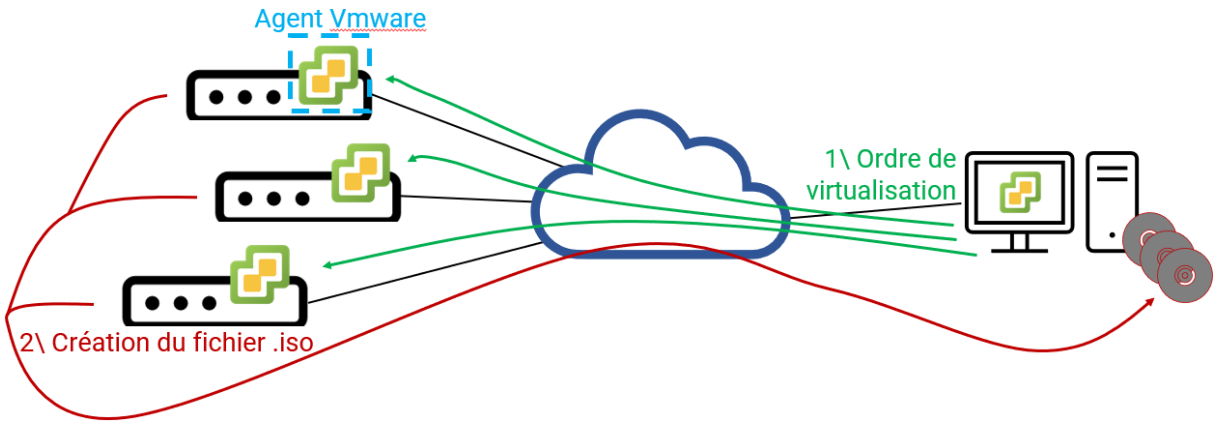


Figure 42 - Création des fichiers .iso

Le schéma précédent illustre le fonctionnement du logiciel VMware, cependant, en pratique, nous sommes confrontés à un problème ; en effet, lors de l'envoi de l'ordre aux esclaves, l'agent installé sur les serveurs met aux alentours de trois minutes à démarrer. De manière générale, Windows tue les processus ne répondant pas pendant plus de 30 secondes, ce qui rend alors le lancement de l'agent impossible.

Pour pallier ce problème, il faut modifier la clé de registre Windows qui gère le temps donné aux processus avant d'être tué en cas d'absence de réponse.

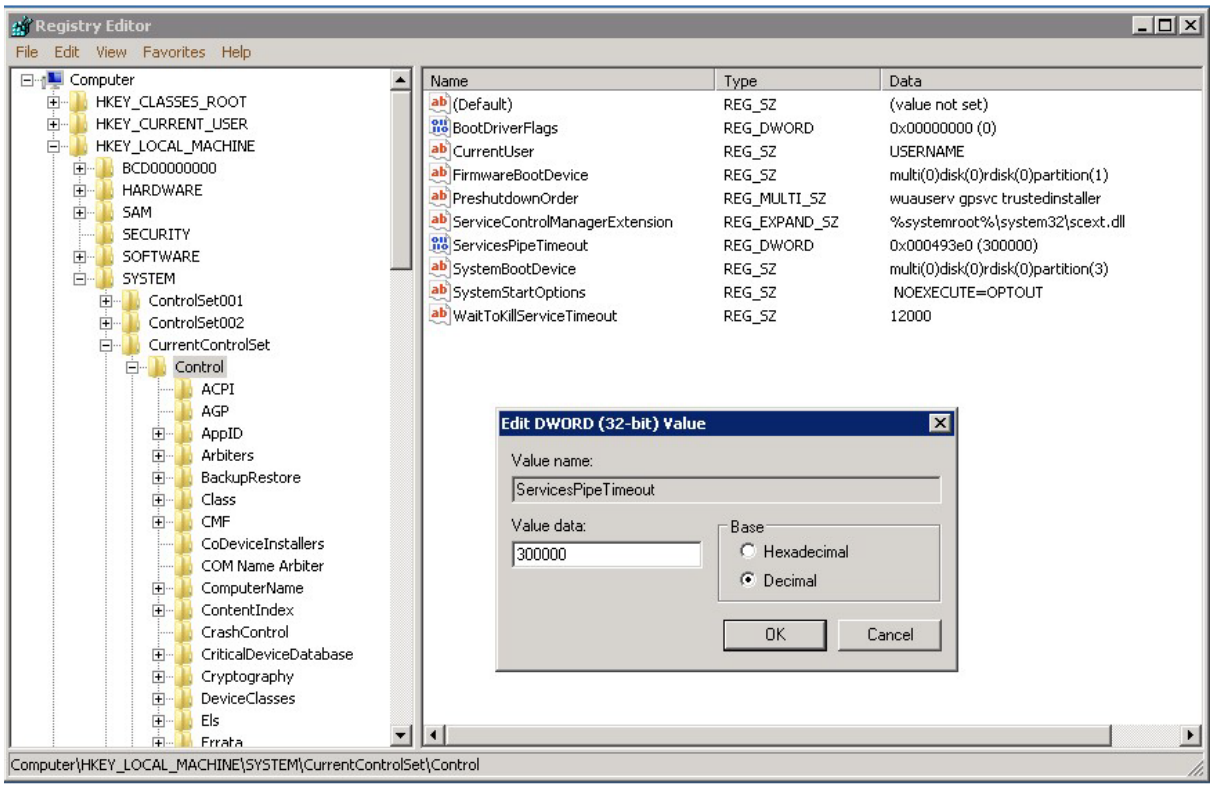


Figure 43 - Modification de la clé de registre ServicesPipeTimeout

Ici, la valeur est modifiée à 300 000ms, soit 5 minutes, ce qui devrait laisser amplement le temps a l'agent VMware de répondre à Windows afin de ne pas être tué.

Malheureusement la modification de clés de registre implique systématiquement un redémarrage de la machine pour être prise en compte ce qui ralentit indirectement la vitesse de notre P2V, car un arrêt de serveur passe forcément par plusieurs procédures internes.

Après la modification de la clé de registre ainsi que le redémarrage du serveur, nous pouvons recommencer la création des fichiers ISO.

Lors du lancement, l'agent esclave va récupérer toutes les informations relatives au serveur qu'il présente ensuite au maître, ce dernier aura la possibilité de confirmer les informations avant le démarrage de la création du fichier ISO.

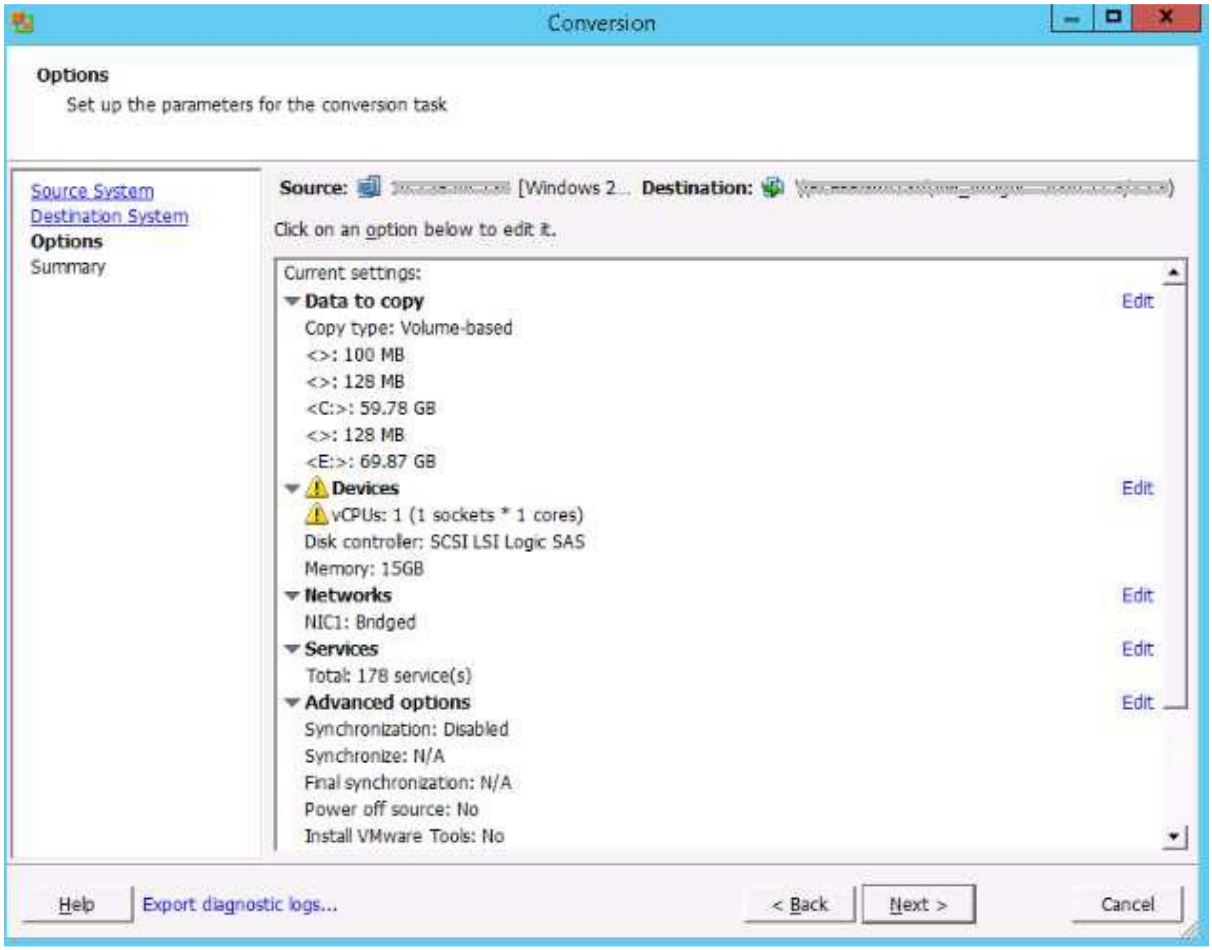


Figure 44 - Récapitulatif avant création de l'ISO

Ici, nous pouvons constater que l'agent a détecté deux disques, 15 Go de RAM, 178 services et une anomalie sur les processeurs qu'il n'a pas réussi à récupérer. Ce n'est pas grave puisque nous pouvons lui indiquer nous-mêmes le nombre de cœurs du serveur à l'aide du bouton d'édition.

Une fois les informations confirmées, la création du fichier ISO commence, cette dernière, en fonction de la taille du serveur, peut varier entre 45 minutes et 3 heures.

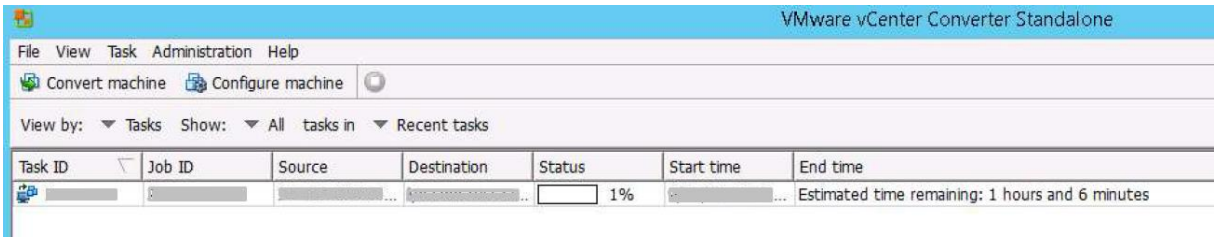


Figure 45 - Création du fichier ISO

Une fois la création terminée, il suffit d'importer le fichier dans notre infrastructure Nutanix en tant que CD-ROM d'installation.

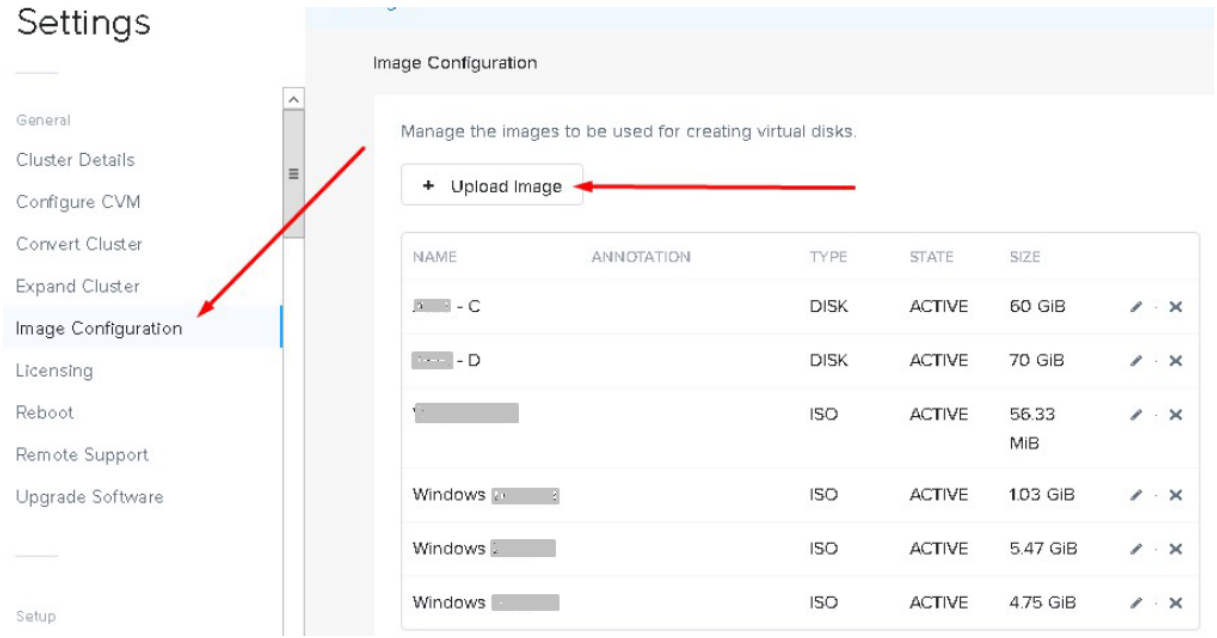


Figure 46 - Images disponibles dans Nutanix

Ainsi, il ne nous reste plus qu'à créer une nouvelle VM comme vu précédemment, cependant, à l'étape du choix du système d'exploitation installé, nous ne choisirons pas une version de Windows, mais le fichier ISO du serveur concerné.

Une dernière étape vient s'ajouter, en effet, une fois la VM crée, lors de son démarrage, elle va virtualiser et mettre en ligne un clone du serveur physique sur le réseau. Ceci est alors problématique, car le serveur physique est quant à lui, toujours en ligne, en conséquence, lors du démarrage de la VM, il y aura un conflit d'adresses IP entre la version physique et virtuelle du serveur.

Pour pallier ce problème nous pouvons au choix, changer l'adresse IP du serveur virtuel ou alors, éteindre le serveur physique avant de démarrer la VM.

Dans le cas où le serveur possède au minimum un client, c'est-à-dire une machine distante se connectant au serveur par son adresse IP, il sera préférable d'éteindre le serveur physique et de démarrer sa version virtuelle. En effet, un changement d'adresse IP nous obligerait à aller modifier tous les clients du serveur afin d'y renseigner la nouvelle adresse IP.

Lors du passage au virtuel, le serveur physique est arrêté, puis l'équipe Systèmes patiente deux semaines afin de confirmer qu'il n'y a aucune remontée d'erreur. Si c'est bien le cas, le serveur physique est enfin décommissionné de la salle technique et envoyé au recyclage.

Comme nous pouvons le constater, le P2V est beaucoup plus contraignant, en effet, il nécessite un nombre supplémentaire d'étapes ainsi que l'obligation de redémarrer les serveurs visant à être virtualisés.

2.7.3\ Sauvegarde

Nutanix permet l'utilisation de « templates » de sauvegarde, c'est-à-dire que chaque VM a la possibilité d'être affectée à un template de sauvegarde qui obéira à des règles différentes renseignées en amont.

Chaque serveur possède un indice de criticité différent, il existe en effet des serveurs où il est impossible de tolérer la moindre perte de données, alors que nous pouvons êtes moins exigeants pour d'autres.

En conclusion, nous pouvons appliquer différentes politiques de sauvegarde en fonction de l'importance du serveur et, afin d'éviter d'avoir à renseigner pour chaque serveur les différents paramètres de sauvegarde, il est plus pratique de créer un template où seront renseignés tous les paramètres et d'associer ce dernier à une VM.

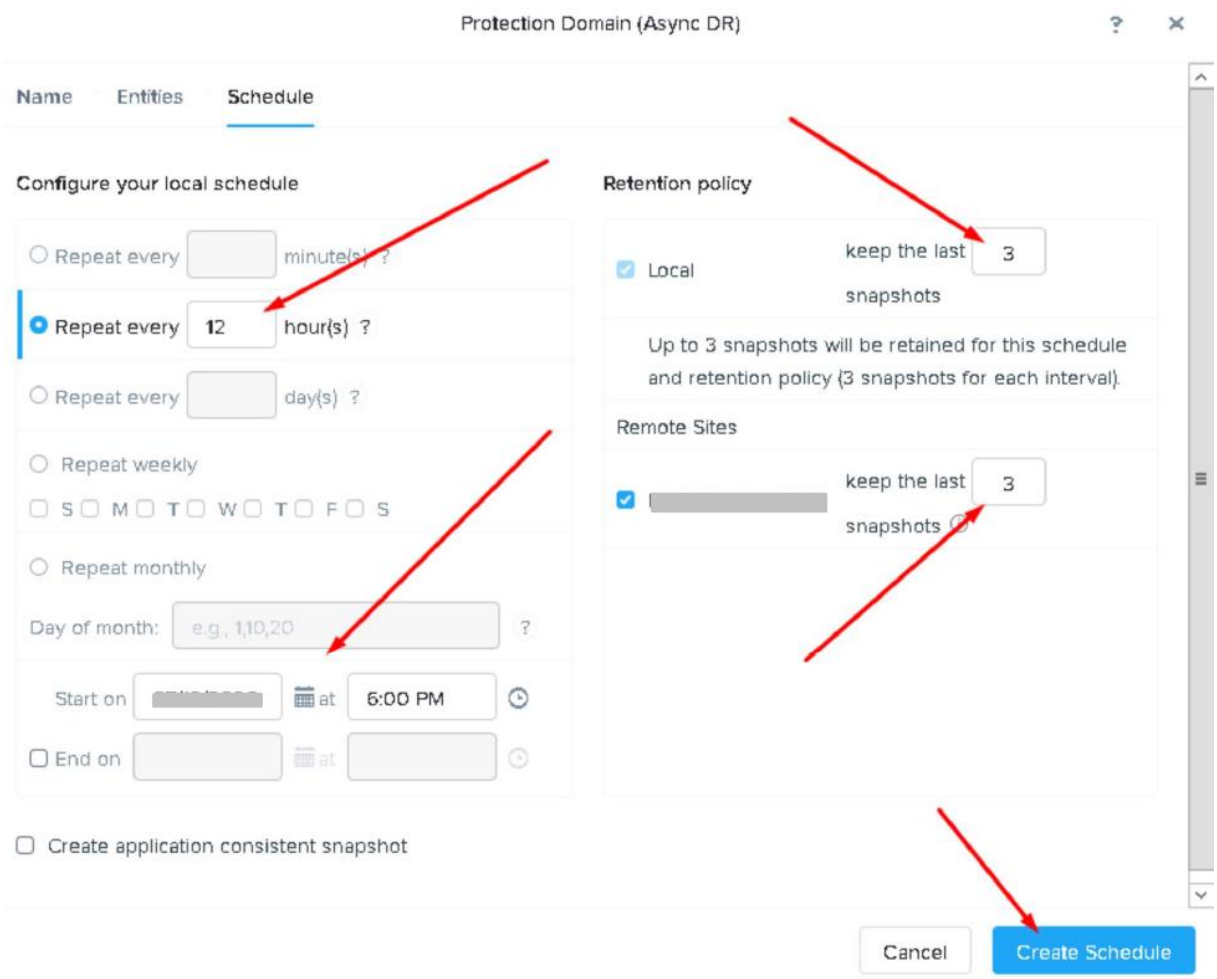


Figure 47 - Template de sauvegarde

La figure précédente illustre un template, nous pouvons observer que toutes les 12 heures, j'effectue une copie de la VM vers l'autre nœud et que je garde, aussi bien localement que sur le nœud distant, 3 sauvegardes.

En conclusion, chaque VM rattachée à ce template possède une sauvegarde avec un delta de 12, 24 et 36 heures sur les deux nœuds dans le cas où nous souhaitons effectuer des retours à l'ancien état à un moment clé de la journée.

Au moment de la 4e sauvegarde, chaque nœud supprime la sauvegarde la plus ancienne, car que nous n'en conservons que 3 afin de limiter les ressources d'espace disque nécessaires.

Enfin, j'associe chaque VM concernée par mon template à ce dernier.

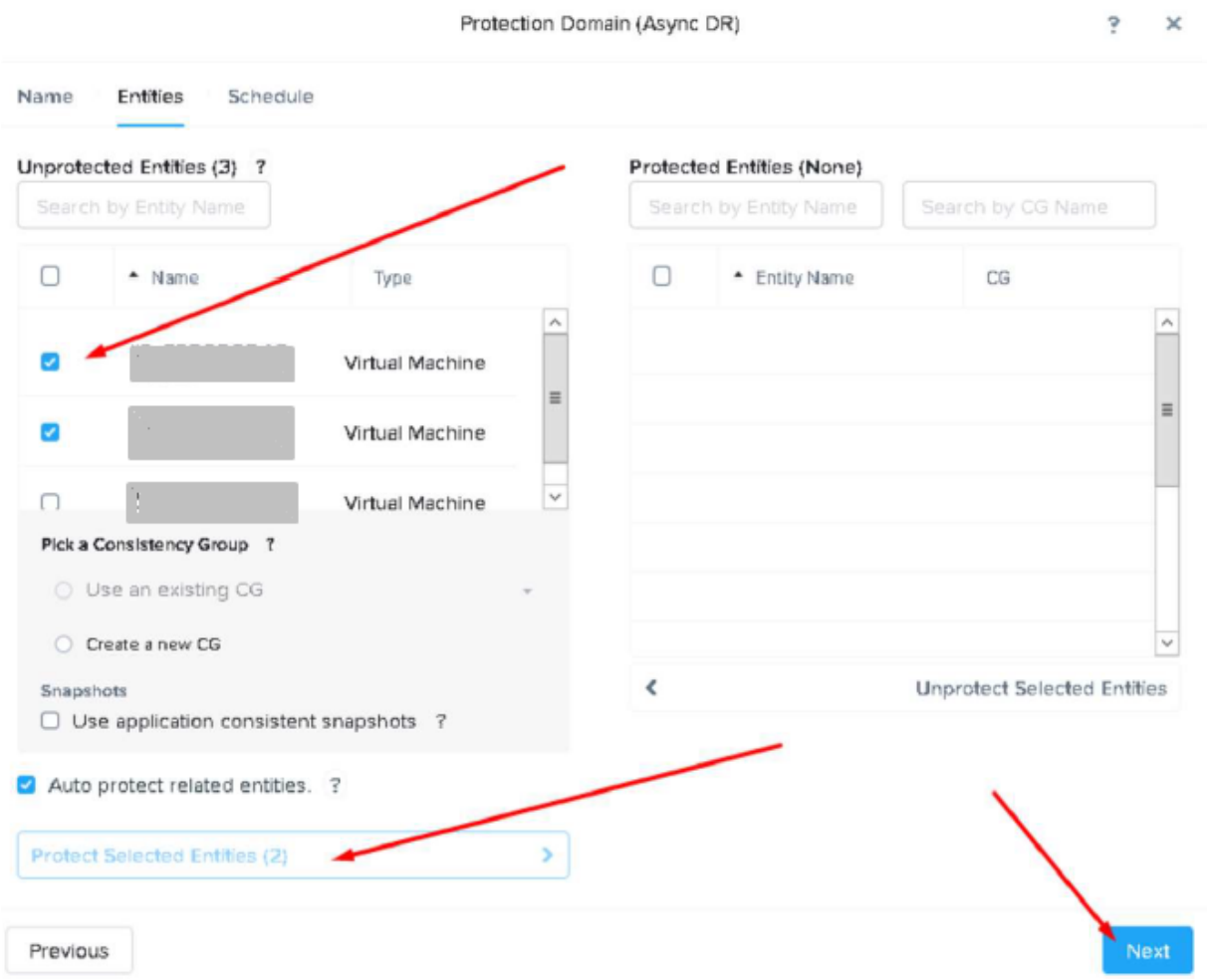


Figure 48 - Association des VMs au template

3\ Axe d'amélioration

Avec la clôture du chapitre précédent, le projet de virtualisation de la plateforme de Grandpuits-Gargenville est terminé ; en effet, tous nos serveurs physiques sont virtualisés et les salles techniques sont vidées des serveurs physiques ainsi que de la baie SAN.

A cet instant, il ne reste plus qu'à effectuer le recettage et corriger les quelques potentiels évènements liés à cette nouvelle infrastructure.

Dans ce chapitre, nous allons nous intéresser à un axe d'amélioration qui pourrait être intégré à court terme dans nos nouveaux systèmes d'information.

Dans ce présent document, lors du détail technique de la commutation du cœur de réseau SII, nous avons souligné le faible débit de ce dernier qui est actuellement en 1Gb/s. Pour rappel, ce faible débit sature rapidement le réseau, ce qui résulte en la perte de paquets IP en cas de trafic intense.

La solution qui nous est venue en tête directement a été de planifier un projet où nous pourrons acheter deux nouveaux routeurs pouvant assurer un débit de 10Gb/s en remplacement des cœurs de réseau actuels. Cette solution, bien que simple, possède l'avantage de régler rapidement le problème en échange d'un cout budgétaire.

Mais, avec l'aide de la technologie « Virtual Routing and Forwarding » (VRF), il est possible de résoudre le problème sans devoir acheter de nouveaux équipements. Cependant, cette technologie complique rapidement les architectures réseau et demande ainsi des qualifications plus avancées dans le domaine du routage.

La technologie VRF permet à plusieurs instances d'une table de routage de coexister dans le même routeur au même instant. En réalité, c'est comme si un seul routeur physique était, sur un plan logique, plusieurs routeurs. Cela signifie alors que, bien qu'elles soient sur le même routeur physiquement, les tables de routages sont en réalité parfaitement cloisonnées et ne possèdent aucun moyen de communiquer entre elles.

Cette solution, par le biais des instances de routage indépendantes, permet alors aux plages IP se chevauchant, ainsi qu'aux adresses IP identiques de coexister sur le même équipement physique sans conflits.

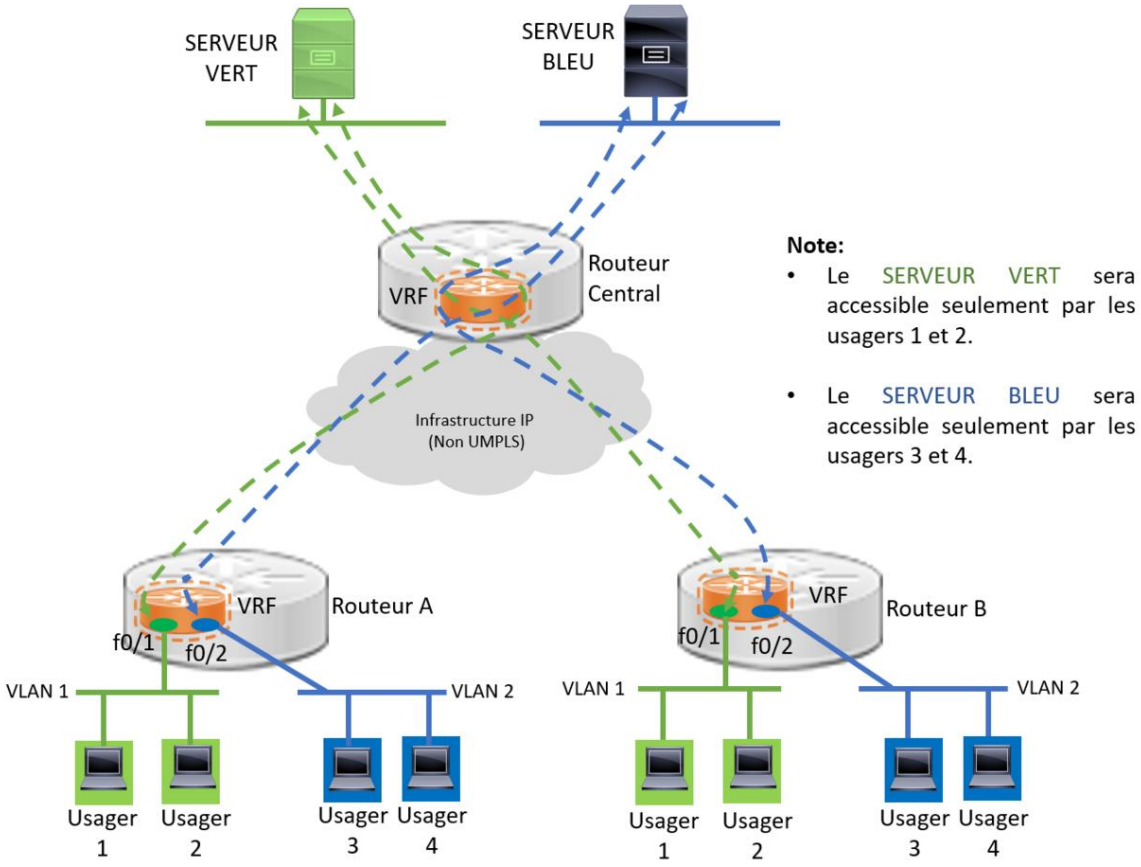


Figure 49 - Explication du fonctionnement VRF (Schéma de fr.wikipedia.org, source en bibliographie).

Le schéma précédent illustre parfaitement le fonctionne de VRF, nous avons deux réseaux, vert et bleu coexistant sur les mêmes routeurs, mais n'ayant aucun moyen de passer d'un réseau à un autre. Ainsi, nous pouvons alors porter plusieurs réseaux avec les mêmes équipements tout en assurant l'isolement de ces derniers.

Grâce à cette technologie, une nouvelle solution s'offre à nous pour le routage du réseau SII. En effet, étant donné que les réseaux VRF sont correctement cloisonnés, il est théoriquement possible de porter le routage SII sur le cœur de réseau SIE.

Cette modification topologique nous permettrait alors de nous séparer des deux routeurs 1Gb/s du réseau SII et ainsi de résoudre notre problème de débit.

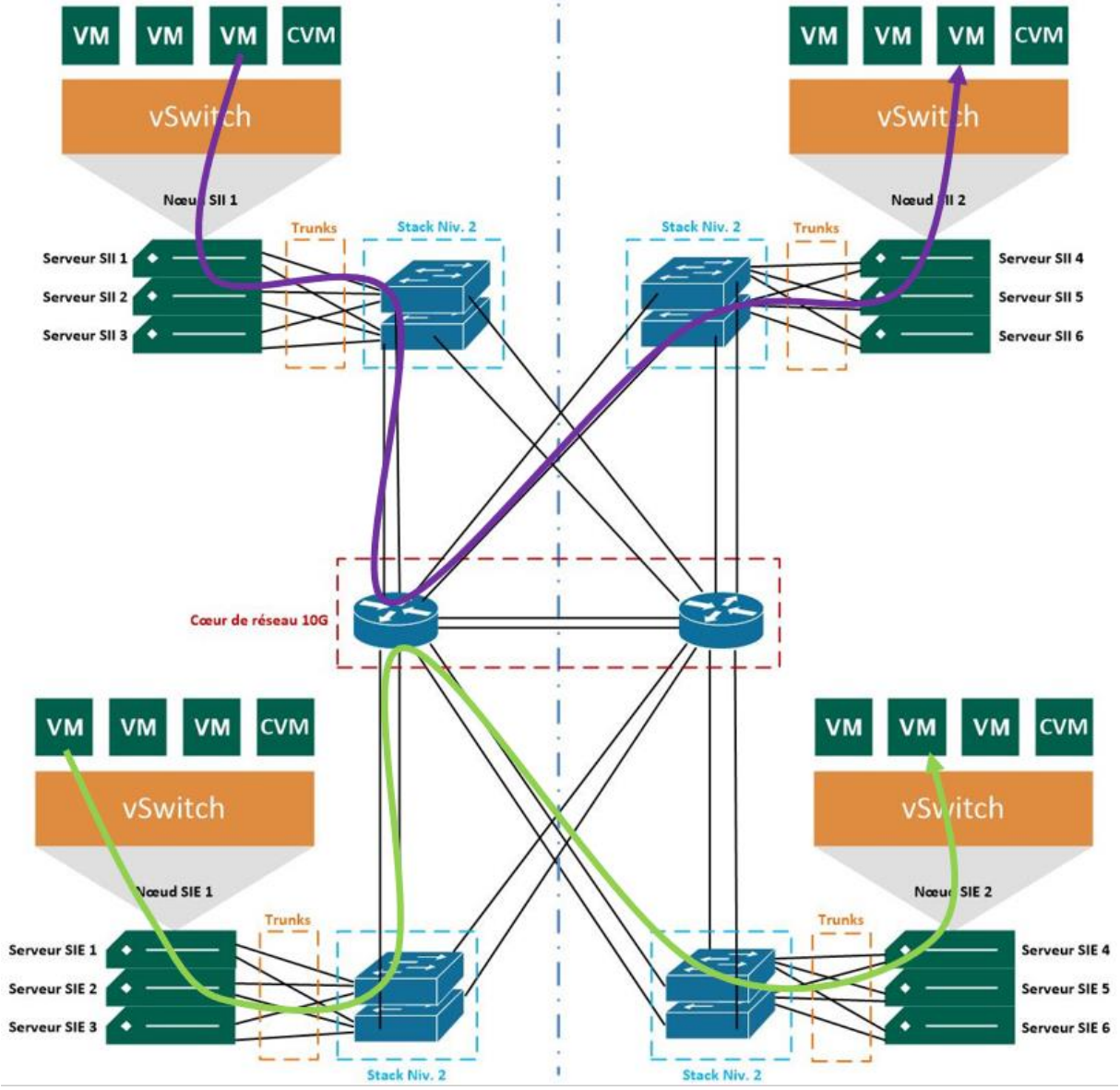


Figure 50 - Schéma des systèmes d'information avec VRF

Comme nous pouvons le constater, cette solution permet au cœur de réseau SIE d'être responsable du routage des systèmes d'information tout en assurant un isolement entre eux ; ils ne peuvent en aucun cas communiquer ensemble .

Pour simplifier, vu que nous avons 2 instances de table de routage, virtuellement c'est comme si chaque routeur physique était en réalité 2 routeurs virtuels n'ayant aucun lien permettant de communiquer. Virtuellement, nous avons donc 4 routeurs, à savoir 2 pour le SIE ainsi que 2 autres pour le SII.

Cependant, comme vu précédemment, il est possible que dans certains scénarios les VMs des réseaux SII et SIE aient besoin de communiquer entre eux. Pour rappel, d'après l'ANSSI il est impératif d'isoler les réseaux SIE et SII, mais il est autorisé que les deux réseaux communiquent entre-deux tant que les flux passent par des pare-feux DMZ.

Or, dans notre infrastructure VRF, les réseaux sont complètement hermétiques et empêchent cette communication, c'est d'ailleurs pour cette raison que nous avons implémenté la technologie VRF ; mais nous avons quand même besoin d'ouvrir une route entre les deux réseaux pour certains flux tout en respectant les recommandations de l'ANSSI.

Il est alors possible d'utiliser des « fuites de routes », il s'agit ici d'un moyen de faire fuiter les routes d'une instance de table de routage à une autre afin que cette dernière apprenne alors les routes que nous voulons faire fuiter.

Sur les routeurs de la marque Cisco, la fuite de route s'effectue grâce au protocole de routage dynamique « Border Gateway Protocol » (BGP) ; en effet, les fuites de route sont effectuées au niveau du processus BGP. Pour cette raison il est nécessaire d'utiliser ce protocole alors que nous ne sommes pas un contexte topologique d' « Autonomous system » (AS).

Afin d'effectuer correctement une fuite de route, il faut dans un premier temps configurer une « route-map » dans laquelle nous allons définir les réseaux ayant pour but d'être fuités vers l'autre instance de routage.

Dans notre cas, nous allons simplement faire fuiter les réseaux de destinations SII et SIE vers des firewalls DMZ.

Une fois cette route-map crée, sur les routeurs en ligne de commande, nous créons un routeur bgp qui redistribuera la route-map contenant les routes fuitées.

Tableau IV - Commandes création d'un routeur BGP

```
route-map SII permit 10
!
router bgp 1
  address-family ipv4 unicast
    redistribute [protocole] 1 route-map SII
```

Une fois les routes fuitées d'une VRF, elles sont accessibles par l'autre VRF, il reste cependant à les importer afin de les prendre en compte dans l'instance de routage.

Tableau V - Commande importation d'une VRF

```
import vrf SIE map SII
```

Cette dernière commande tapée, la fuite de route d'une VRF à l'autre est effectuée, il ne reste plus qu'à faire les mêmes manipulations dans l'autre sens, en l'occurrence de SII vers SIE.

En conclusion, si un paquet IP souhaite passer du réseau SIE à SII, il sera routé par la VRF SIE vers le cluster de pare-feux DMZ, ce dernier va faire changer le paquet IP de zone de sécurité puis le renvoyer vers le cœur de réseau ; cependant, il arrivera dans la VRF SII et aura, par conséquent, changé de réseau.

Nous retrouvons ainsi notre fonctionnement précédent, c'est-à-dire deux réseaux complètement cloisonnés avec comme seule possibilité de communication un lien passant par des pare-feux DMZ.

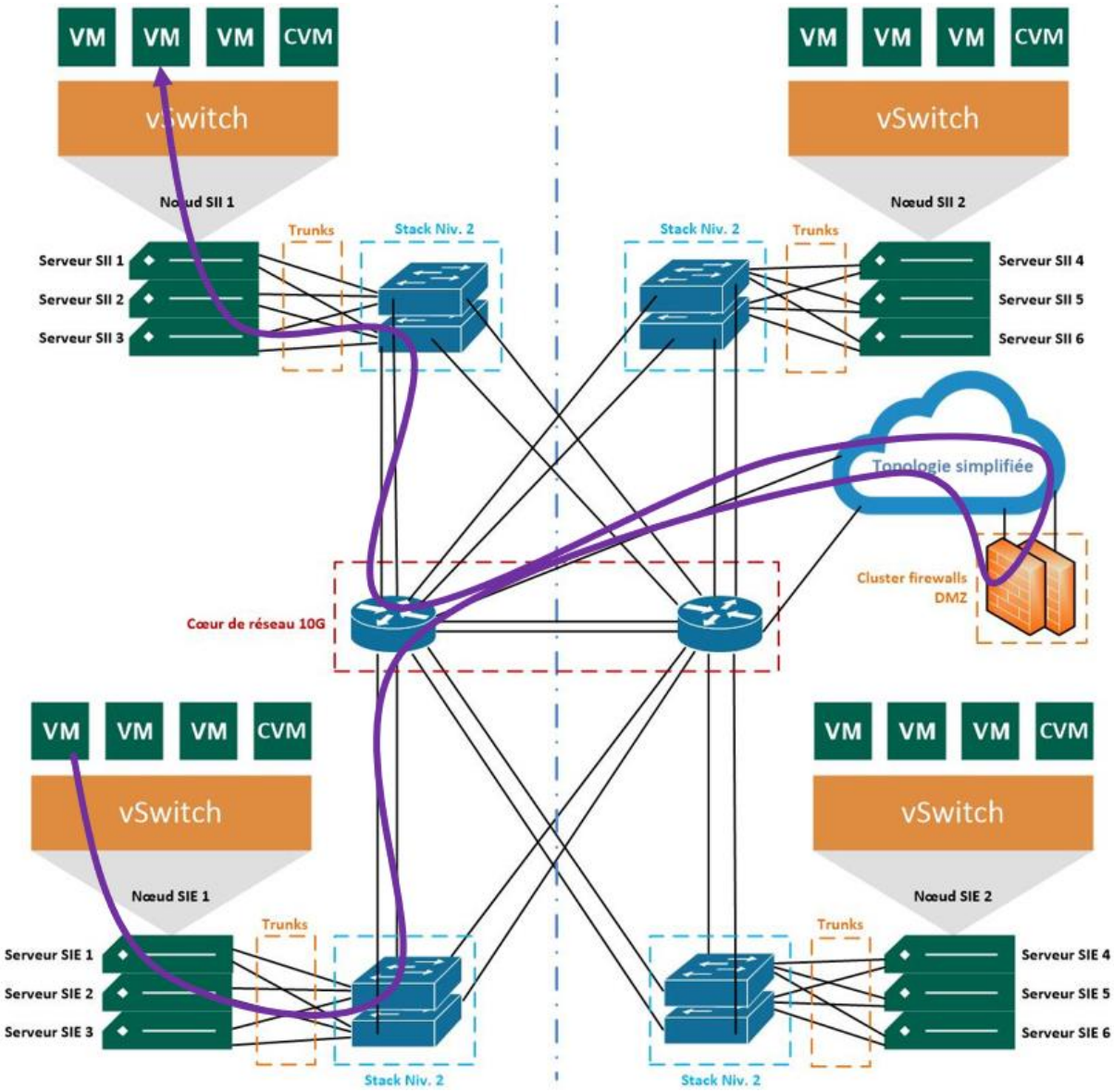


Figure 51 - Architecture VRF + Fuites de routes

Nous pouvons vraiment constater que l'implémentation des VRF complique fortement l'architecture, mais nous permet d'éviter de nouveaux investissements.

Enfin, il tient bon de rappeler que l'ANSSI tolère l'utilisation des VRF, mais ne recommande pas que cette technologie soit la seule méthode de cloisonnement du système d'information ; ce qui n'est effectivement pas le cas dans nos systèmes d'information.

4\ Retour d'expérience

Au sein de la plateforme de Grandpuits-Gargenville, j'ai pu mettre en pratique de nombreuses connaissances que j'ai apprises durant mon parcours académique au CNAM.

En effet, les cours de management de projet m'ont été d'une grande utilité par ma position dans le projet. J'ai ainsi pu mettre en pratique toutes les bonnes méthodes de management de projet qui m'ont été enseignées au CNAM.

Par exemple, j'ai utilisé différentes matrices afin d'évaluer l'influence, l'impact ainsi que l'intérêt des parties prenantes dans ce projet afin d'identifier correctement quelles personnes seront les parties prenantes clés aux différentes étapes du projet.

Aussi, j'ai pu mettre en place une matrice RACI permettant d'identifier clairement le rôle de chacun à tout instant du projet. Enfin, lors de la phase d'achat de la solution de virtualisation, j'ai pu utiliser un tableau d'approvisionnement afin de choisir correctement parmi les solutions retournées par nos prestataires.

Sur un point de vue réseau, j'ai pu confirmer mes compétences dans ce domaine en effectuant des missions comme :

→ La création de nouveaux réseaux et la définition des plages d'adressage IP.
→ La gestion du trafic IP de niveau 2, c'est-à-dire la commutation réseau par le biais de VLANs, Trunks ou encore STP.
→ La modification de pare-feux et ainsi le filtrage des flux de données.
→ La création et la modification d'access-lists permettant de filtrer les trafics de données.
→ Le routage, qu'il soit direct, statique ou dynamique, permettant ainsi aux paquets IP de changer de réseau.
→ L'analyse de la sécurité des réseaux en suivant les recommandations de l'ANSSI dans le but de sécuriser nos systèmes d'information.

De plus, le nouvel environnement étant virtuel, j'ai pu constater que des tâches que j'avais l'habitude d'effectuer étaient plus compliquées dans un environnement virtuel.

Enfin, sur un point de vue système, j'ai pu apprendre énormément de connaissances en matière de virtualisation et de redondances des données.

J'ai en effet pu me rendre compte de l'importance des données et j'ai pu avoir la chance d'installer et de voir les différentes technologies mises en place pour réduire au maximum la perte de données.

Aussi, j'ai pu travailler sur les solutions de virtualisation et ainsi effectuer des tâches comme le P2V, le calcul et l'assignation des ressources à une VM ou encore comme assurer au maximum la disponibilité de cette dernière.

Ce projet englobant à la fois management de projet, réseau et systèmes m'a permis de progresser et d'approfondir mes connaissances dans ces trois domaines.

5\ Conclusion

En conclusion, à ce jour, la plateforme de Grandpuits-Gargenville possède désormais des systèmes d'information à jour ne présentant plus de failles de sécurité.

Ces années au sein de TotalEnergies m'ont été très bénéfiques sur le plan professionnel comme sur le plan personnel.

Professionnellement, j'ai vu mes compétences et connaissances évoluer dans plusieurs domaines. J'ai eu l'occasion de m'investir dans plusieurs spécialités informatiques très différentes tout en les mettant en corrélation : c'est en effet grâce au projet présenté dans ce présent document que j'ai pu progresser dans de multiples domaines de l'informatique.

J'ai énormément appris des nouvelles architectures virtuelles, en effet, devoir en implémenter une a été pour moi la meilleure façon de comprendre la méthode de fonctionnement. Ces compétences développées dans les architectures virtuelles sont pour moi très précieuses, car en effet, je pense en effet qu'il s'agit du futur de l'informatique. Nous pouvons en effet déjà observer chez des constructeurs comme Cisco, des routeurs virtuels (XRv), c'est donc pour moi une chance d'avoir pu m'améliorer dans ce monde de l'informatique.

Aussi, j'ai beaucoup appris sur le relationnel en entreprise, une bonne atmosphère de travail ainsi qu'une cohésion d'équipe sont des valeurs très importantes à TotalEnergies. J'ai travaillé avec un certain nombre de parties prenantes lors de mes missions, en effet, pour le projet auquel j'ai été affecté, un grand nombre de personnes étaient concernées par ce dernier, il fallait garder tout le monde au courant des changements et surtout veiller à l'implication de l'équipe dans le projet.

J'ai eu l'honneur de pouvoir participer à un projet de son commencement à sa fin, c'est-à-dire de l'analyse fonctionnelle jusqu'au recettage. J'ai même pu participer à des phases clés en autonomie comme la rédaction du cahier des charges, l'appel d'offres, la consultation et la clarification technique, l'achat de la solution, la réception, son installation ainsi que sa mise en œuvre.

J'ai eu la chance de pouvoir mettre en œuvre et pousser mes compétences acquises lors de mes cours au CNAM en participant à ce projet. En effet, j'ai pu développer mes compétences en gestion de projet, réseaux et systèmes qui sont, pour moi, les qualités d'un ingénieur en informatique.

Sur le plan personnel, prendre part à une équipe déjà en place et interagir avec mes collègues, ma hiérarchie et les autres équipes m'a permis d'avoir une plus grande confiance en moi, et d'être plus clair face à un public possédant des connaissances et compétences différentes.

Enfin, je suis ravi d'avoir été accueilli et intégré dans une équipe aussi soudée et joviale, rendant mon environnement de travail bien plus agréable et certainement plus efficace.

Pour conclure, cette expérience enrichissante m'a motivé à poursuivre mon but professionnel de devenir ingénieur en informatique, c'est pourquoi ce présent document vous est parvenu. Ce mémoire marque l'aboutissement de ma formation d'ingénieur au CNAM ; cette dernière m'a permis d'être prêt à devenir ingénieur en informatique en entreprise.

Références

Nutanix. (2021, Septembre 21). *architecture-de-nutanix-virtual-computing-platform*. Récupéré sur vstory.fr: https://vstory.fr/architecture-de-nutanix-virtual-computing-platform/

TotalEnergies. (2021, Septembre 3). Récupéré sur grandpuits.totalenergies.fr: https://grandpuits.totalenergies.fr/

TotalEnergies. (2021, Septembre 3). *lenergie-se-reinvente*. Récupéré sur totalenergies.com: https://totalenergies.com/lenergie-se-reinvente/

TotalEnergies. (2021, Septembre 3). *resultats*. Récupéré sur totalenergies.com: https://totalenergies.com/fr/actionnaires/resultats-et-presentations-investisseurs/resultats

TotalEnergies. (2021, Septembre 4). *totalenergies-plus-100-00-employes-plus-130-pays*. Récupéré sur totalenergies.com: https://totalenergies.com/fr/infographies/totalenergies-plus-100-000-employes-plus-130-pays

VMware. (2021, Octobre 18). *fr/products/converter.html*. Récupéré sur vmware.com: https://www.vmware.com/fr/products/converter.html

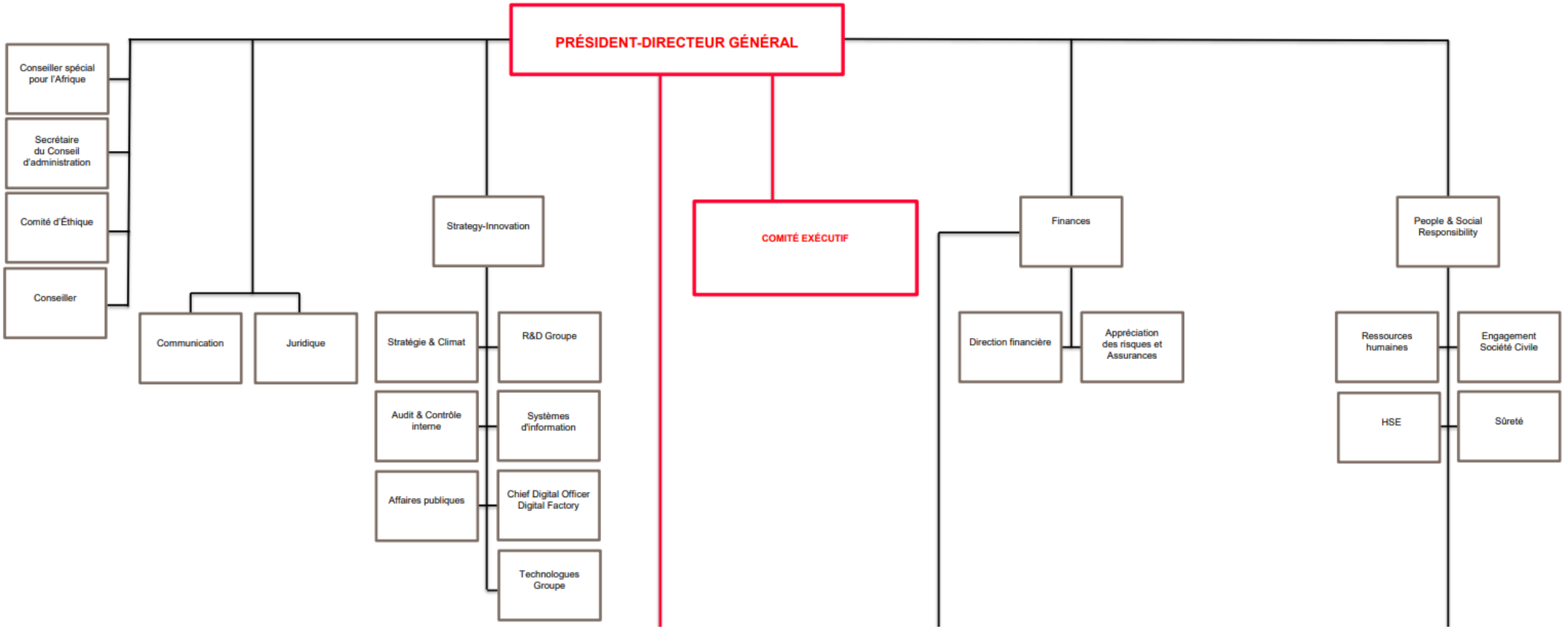
VMware. (2021, Octobre 11). *s/article/64993*. Récupéré sur kb.vmware.com: https://kb.vmware.com/s/article/64993

Wikipédia. (2021, 10 21). */wiki/Virtual_routing_and_forwarding*. Récupéré sur wikipedia.org: https://fr.wikipedia.org/wiki/Virtual_routing_and_forwarding

Wikipedia. (2021, Septembre 29). *fibre_optique*. Récupéré sur wikipedia.org: https://fr.wikipedia.org/wiki/Fibre_optique

Annexes

Organigramme complet 1/2



Organigramme complet 2/2

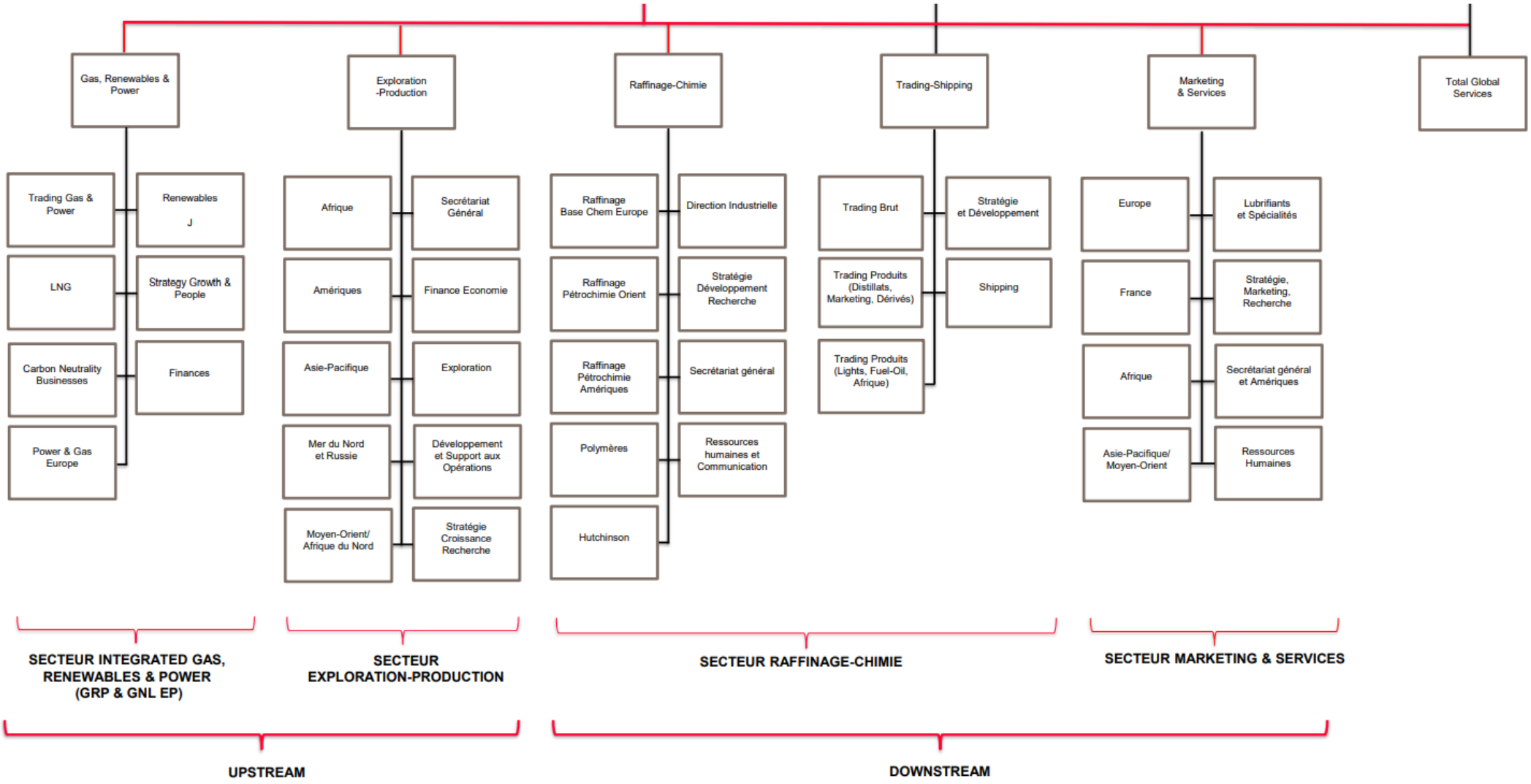


Schéma complet du raffinage

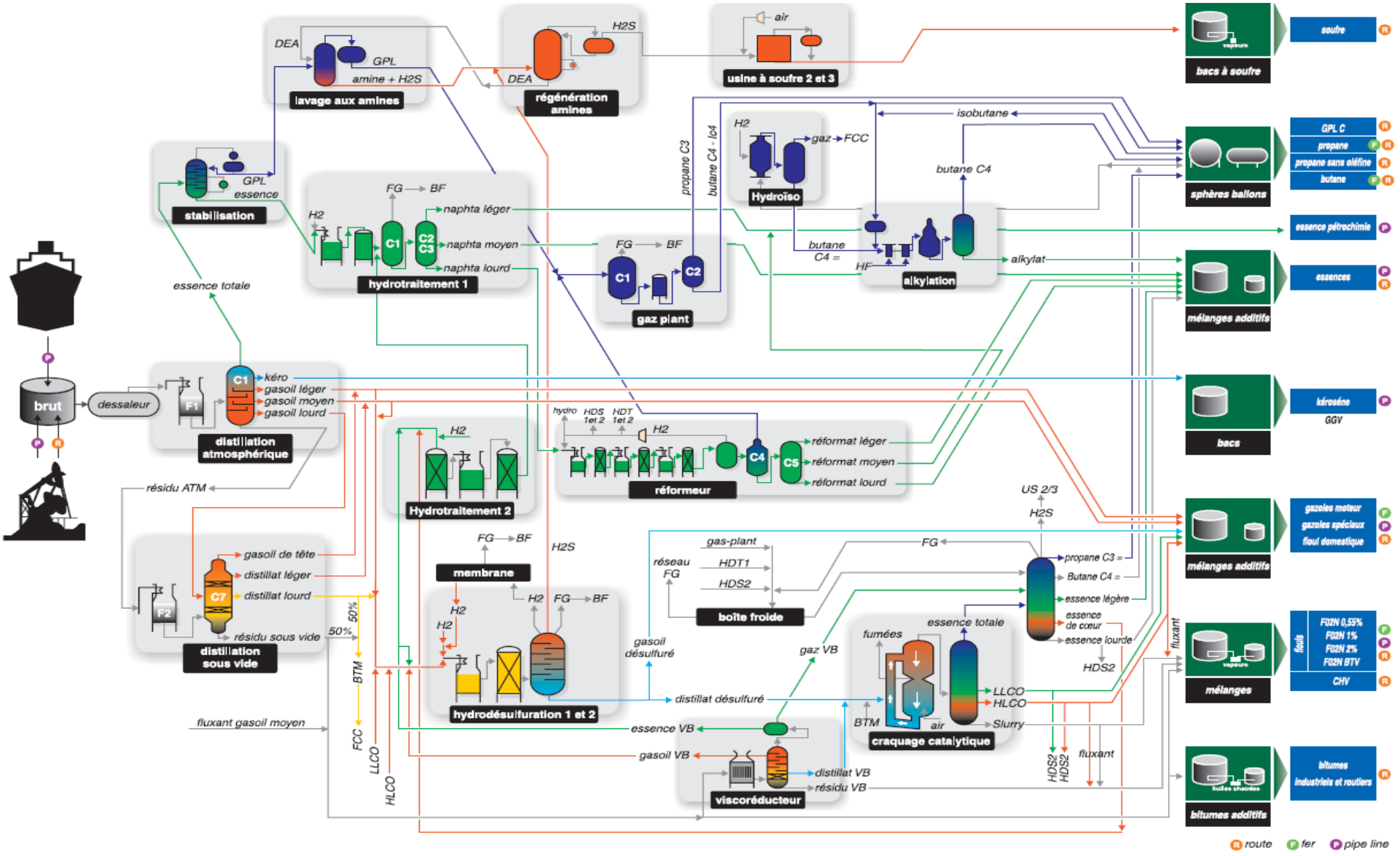


Schéma de solution Nutanix

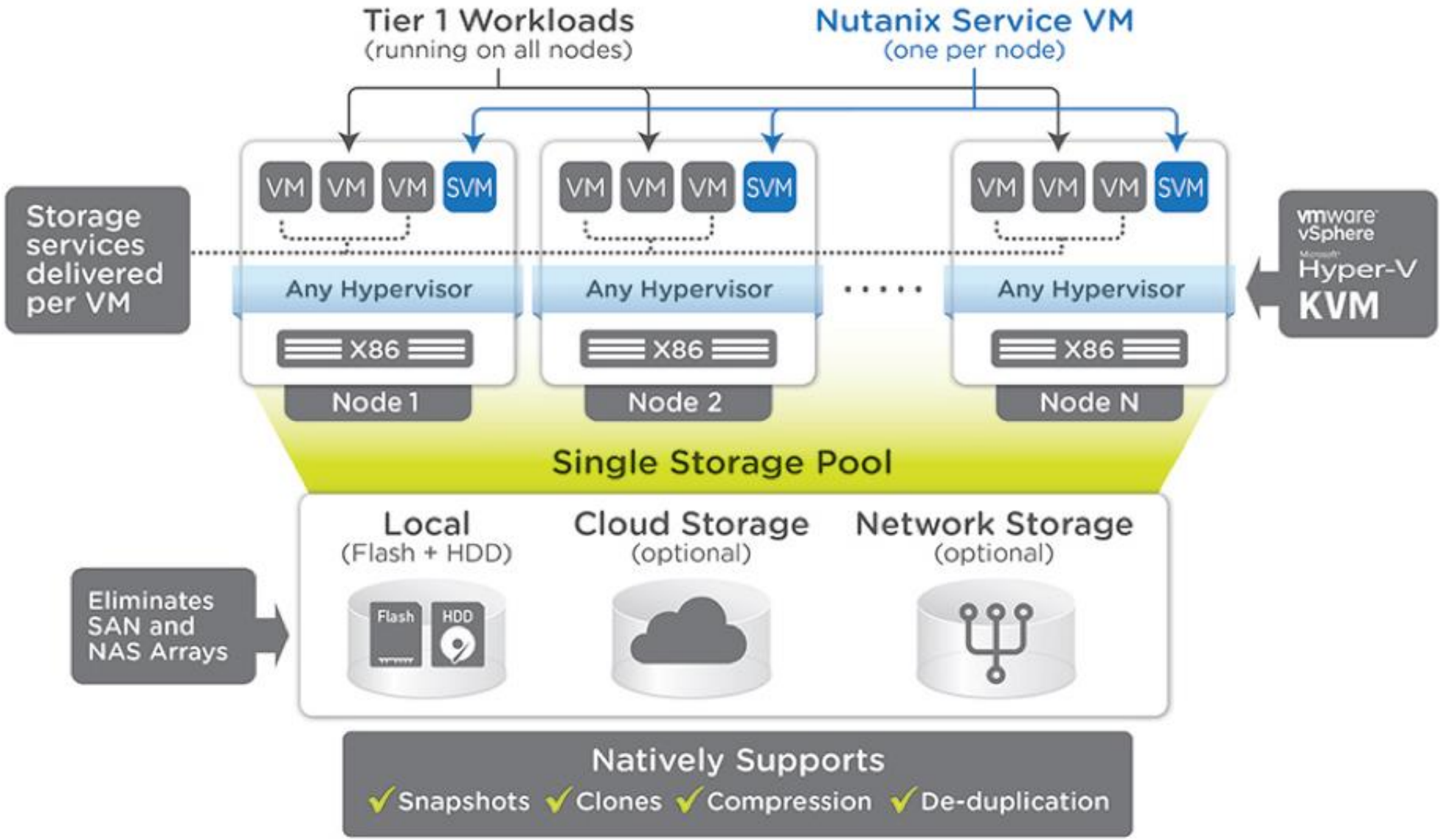
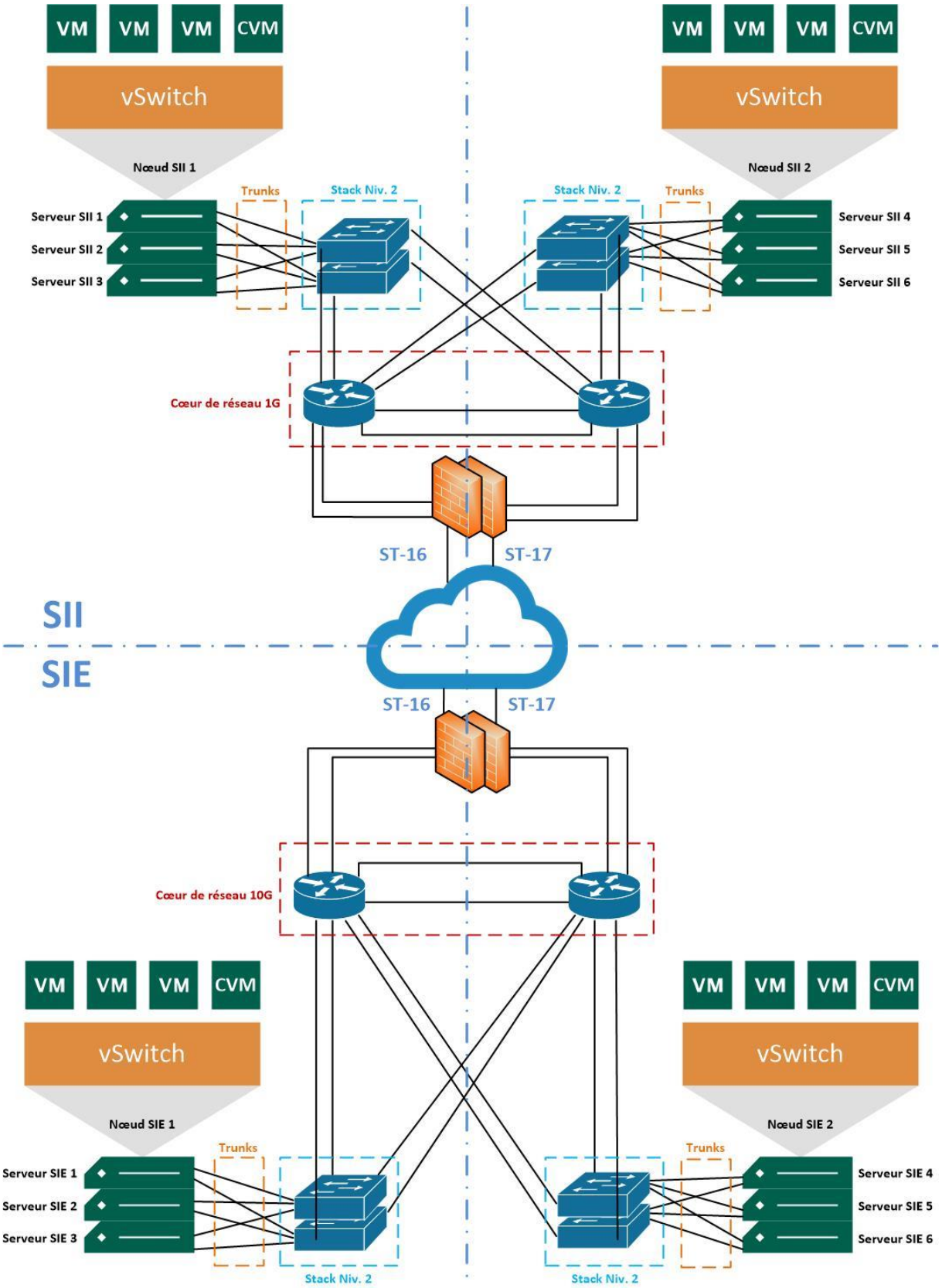


Schéma complet des systèmes d'information



Abstract

TotalEnergies, acteur majeur de l'énergie possède de nombreuses installations pour mener à bien ses différentes missions. Parmi ces installations, la Plateforme de Grandpuits-Gargenville réunissant à la fois une raffinerie et un dépôt de pétrole souhaite mettre à jour son système d'information devenu obsolète. Ce présent document récapitule ma mission d'une durée de deux ans au sein de cette plateforme.

Les technologies de virtualisation étant de plus en plus populaires, c'est tout naturellement que nous nous sommes dirigés vers des solutions de virtualisation pour mettre à jour le système d'information.

Cette mission englobe de nombreux aspects de l'informatique dans un environnement soumis à des contraintes de sécurité élevées. C'est pourquoi ce présent document détaille des concepts réseaux comme la commutation, le routage ou encore la cybersécurité ainsi que des concepts systèmes liés à la virtualisation et la réplication des données.

Mots-clés : Redondance, routage, commutation, gestion de projet, virtualisation, cybersécurité, réplication, sauvegarde, réseaux, systèmes.

TotalEnergies, a major company in energy, has numerous facilities to carry out its various missions. Among these facilities, the Grandpuits-Gargenville Platform, which brings together both a refinery and an oil depot, wishes to update its information system, which has become obsolete. This document summarizes my two-year mission within this platform.

As virtualization technologies are increasingly popular, it is only natural that we have turned to virtualization solutions to update the information system.

This mission summarizes many aspects of IT in an environment with high security constraints. Therefore, this document details network concepts such as switching, routing or cybersecurity as well as concepts related to virtualization and data replication.

Keywords: Redundancy, routing, switching, project management, virtualization, cybersecurity, replication, backup, networks, systems.