République Algérienne Démocratique et Populaire
Université Abou Bakr Belkaid– Tlemcen
Faculté des Sciences
Département d'Informatique

Mémoire de fin d'études

pour l'obtention du diplôme de Master en Informatique

Option: *Réseaux et systèmes distribués (R.S.D)*

Thème

Etude et mise en œuvre d'un plan de reprise d'activité (Disaster Recovery Plan)

Réalisé par :

- Imane KHOUANI
- Nesrine BOUALI

Présenté le 04 juillet 2022 devant le jury composé de:

- Dr. SETTOUTI Ahmed Khalid Yassine (Président)
- Dr. ZIANI-CHERIF Salim (Encadrant)
- Mr. BELHOCINE Amine (Examinateur)

Année universitaire : 2021-2022

Remerciements

Nous exprimons d'abord nos sincères remerciements à Monsieur *ZIANI-CHERIF Salim*, Maitre de conférences au département d'Informatique, Faculté des Sciences, Université de Tlemcen, et membre du laboratoire de recherche informatique (L.R.I.), pour nous avoir soutenues tout au long de cette période de mémoire de master, qu'il trouve ici l'expression de toute notre reconnaissance pour la confiance qu'il nous a accordée en acceptant la direction de ce manuscrit. Nous le remercions de la patience dont il a fait preuve à notre égard, de sa générosité et de sa disponibilité à tout moment.

Nous remercions également Monsieur SETTOUTI Khaled de nous faire l'honneur de présider ce jury et Monsieur BELHOCINE Amine d'avoir accepté d'examiner ce travail.

Nos remerciements les plus sincères à Monsieur TOUATI Tarek et Monsieur BENABBOU Zohir exerçant au niveau de l'entreprise « iServ Solutions », pour l'aide inestimable qu'ils nous ont apporté dans la réalisation de ce travail. Qu'ils soient assurés de notre profonde gratitude et haute considération.

Nous tenons à remercier tout le staff du département d'informatique pour l'aide fournie durant tout le cursus universitaire.

Imane KHOUANI

Nesrine BOUALI

Dédicaces

À ma chère maman, mon rayon de soleil et l'hirondelle de mon ciel, ton affection me couvre, ta bienveillance me guide, ton courage m'inspire et ta présence à mes côtés a toujours été ma source de force pour affronter les difficultés de la vie. Je te dédie ce travail qui a été réalisé sous l'aile de ton soutien et de tes encouragements en espérant te rendre fière ne serait-ce qu'un petit peu, que Dieu te garde et te protège.

À mon cher père, rien n'équivaut à nos longs debriefs et discussions profondes si ce n'est tes belles œuvres de bois, je te dédie ce travail et aimerai que tu saches que plus les distances sont grandes, plus les émotions sont fortes, que Dieu te garde et te protège.

À mon petit frère Amine, le sel et le piment de ma vie, nos moments de complicité valent tous les trésors du monde, nos petites chamailleries aussi, que Dieu te garde et te protège.

À mon amie, binôme et âme sœur Nesrine, j'aurais aimé te connaître plus tôt, ta gentillesse, ta sincérité et ton sourire me marqueront à tout jamais, si toute cette expérience était à refaire, j'aimerai que ce soit toujours en ta compagnie. Que ce travail soit le fruit de notre persévérance et de notre amitié, que Dieu te garde et te protège.

À toute ma famille,

À tous ceux qui me sont chers,

À tous ceux qui utilisent la science pour le bonheur et la prospérité de l'humanité,

Je dédie ce modeste travail.

Imane KHOUANI

Dédicaces

Tout d'abord, je remercie ALLAH le tout-puissant qui m'a donné le courage, la force et la capacité d'accomplir ce travail.

Je profite de cette occasion pour adresser mes sincères remerciements :

À ma mère et mon père qui m'ont soutenue et encouragée durant ces années d'études, qui ont partagé avec moi tous les moments d'émotion lors de la réalisation de ce travail, et m'ont chaleureusement supporté et encouragé tout au long de mon parcours.

À mes sœurs, mon frère et sa femme qui m'ont encouragée et m'ont souhaitée du succès dans ma vie

À mes grands-parents, mes tantes pour leurs prières qui m'ont accompagnées, que Dieu leur donne une longue et joyeuse vie.

À ma famille et mes proches.

À tous mes amis sans exception pour leur soutien moral, qui m'ont toujours encouragé « vous êtes ma 2ème famille »

Sans oublier mon amie et binôme Imane je suis très reconnaissante de t'avoir connue, d'avoir été ton binôme, de ton soutien moral, ta patience et ta compréhension, pour tous les moments partagés (stress, fou rire, retard, …) au long de ce projet, mes mots ne peuvent pas exprimer tout ce que je ressens j'aimerais que notre amitié dure jusqu'à la fin, je te souhaite un avenir radieux, que Dieu te garde.

Nesrine BOUALI

Résumé : Le nombre d'entreprises qui s'appuient sur leurs systèmes informatiques pour effectuer leurs opérations quotidiennes s'est développé rapidement et ne cesse de croitre. Les données informatiques d'une entreprise sont des ressources cruciales et critiques qui doivent être protégées contre tout risque lié à la sécurité, aux pertes de données ou bien aux pannes de matériel. Un plan de reprise d'activité (PRA) doit être élaboré afin d'assurer, dans le cas d'une crise majeure au niveau de l'entreprise, la reconstruction de son infrastructure informatique et la remise en route des applications nécessaires à son activité. Ce travail va présenter l'état de l'art d'un plan de reprise après sinistre, la mise en œuvre d'une solution de sauvegarde et de récupération, et la simulation d'un scénario d'interruption et de reprise d'activité.

Mots clés : PRA, entreprise, désastre, reprise, systèmes informatiques, données, risque, sauvegarde.

Abstract: The number of companies that rely on their IT systems to perform their daily operations has grown rapidly and continues to increase. A company's computer data is a crucial and critical resource that must be protected from any security risk, data loss or hardware failure. Therefore, a Disaster Recovery Plan (DRP) must be developed to ensure that, in the event of a major crisis at the enterprise level, the IT infrastructure is rebuilt and the applications necessary for the business are restored. This paper will present the state of the art of a disaster recovery plan, the implementation of a backup and recovery solution, and the simulation of an interruption and recovery scenario.

Keywords: DRP, enterprise, disaster, recovery, IT systems, data, risk, backup.

ملخص: يزداد عدد الشركات التي تعتمد على أنظمة تكنولوجيا المعلومات الخاصة بها لأداء عملياتها اليومية بسرعة. تعد بيانات الكمبيوتر الخاصة بالشركة موردًا حاسمًا يجب حمايته من أي مخاطر مرتبطة بالأمان أو فقدان البيانات أو فشل الأجهزة. لذلك وجب تطوير خطة للتعافي من الكوارث(PRA) ، لضمان إعادة بناء البنية التحتية لتكنولوجيا المعلومات واستعادة التطبيقات اللازمة لأعمال الشركة في حالة حدوث أزمة كبيرة على مستوى المؤسسة. سيقدم هذا العمل مميزات واستراتيجيات خطة التعافي من الكوارث، كيفية تنفيذ حل نسخ واسترجاع المعلومات، ومحاكاة سيناريو انقطاع ثم استعادة نشاط المؤسسة.

الكلمات المفتاحية: خطة التعافي من الكوارث، شركة، خطر، كارثة، نسخ، استرجاع، البيانات، أنظمة تكنولوجيا المعلومات.

Table de matières

INTRODUCTION GENERALE **9**

CHAPITRE I TERMINOLOGIE, CARACTERISTIQUES ET ETAT DE L'ART D'UN PLAN DE REPRISE D'ACTIVITE (PRA) **11**

I.1. Introduction **12**

I.2. Définition **12**

I.3. Cycle de vie d'un PRA **13**

I.4. Étude de risque **14**

I.4.1. Étapes d'une étude de risque 14

I.5. Périmètre d'un PRA **20**

I.6. Sauvegardes **21**

I.7. Stratégies du PRA **22**

I.7.1. Utilisation d'un site de reprise 22

I.7.2. Stratégie basée sur le Cloud (Cloud DR) 23

I.7.3. Stratégie basée sur le DRaaS (PRA as a Service) 23

I.8. Bibliographie des architectures **23**

I.8.1. Etude comparative de topologies réseaux des centre de données 25

I.8.2. Architectures et topologies proposées 27

I.9. Conclusion **31**

CHAPITRE II OPTIMISATION D'OBJECTIFS DE REPRISE **32**

II.1. Introduction **33**

II.2. Architecture initiale de l'entreprise « X » **33**

II.2.1. Composantes de l'architecture 34

II.2.2. Contraintes et limitations de l'architecture 35

II.3. Architecture optimisée 36

II.4. Conclusion 39

CHAPITRE III REPRISE D'ACTIVITE APRES SINISTRE EN UTILISANT RELAX AND RECOVER 40

III.1. Introduction 41

III.2. Outils et simulation 41

III.2.1. Définition 41

III.2.2. Configurer la sauvegarde ReaR avec la méthode NFS 41

III.3. Conclusion 55

CONCLUSION GENERALE 56

BIBLIOGRAPHIE 57

LISTE D'ABREVIATIONS 60

LISTE DES FIGURES 61

LISTE DES TABLEAUX 62

LISTE DES ANNEXES 62

Avant-propos

Comme il apparaitra dans le courant de ce rapport, la thématique étudiée a pour objet une manipulation circonstancielle d'un système informatique, plus ou moins conséquent, avec ses équipements, ses codes et ses données.

Or la problématique ciblée touche par essence des systèmes informatiques appartenant à des entités administratives ou opérateurs économiques dont les ressources ainsi que les architectures sont à caractère confidentiel.

Il en découle que nos interventions restent limitées à certaines opérations tout comme on a souvent recourt à une désignation d'une architecture et d'un système informatique réels « anonyme ».

Cela explique un certain nombre de difficultés pratiques ainsi qu'un certain nombre de limitations d'implémentations réelles, qui nous ont amené à nous suffire de simulations, quand nos partenaires ne peuvent autoriser des manipulations en cas réel.

Nous espérons néanmoins démontrer la faisabilité de notre travail avec une relative maitrise des technologies, architectures ou outils mis en œuvre.

Introduction générale

Aujourd'hui, de nombreux secteurs d'activité sont en partie ou entièrement informatisés. Ainsi, de nombreuses entreprises deviennent progressivement dépendantes de leurs systèmes d'information. Dans un tel contexte, il est facile de comprendre pourquoi la majorité des responsables s'inquiètent beaucoup de l'interruption 'accidentelle' des activités de leurs sociétés. Tout incident ou défaillance peut compromettre la productivité et la rentabilité d'une entreprise.

Les attaques informatiques, les erreurs humaines et les sinistres sont des phénomènes qui peuvent se montrer aussi ravageurs qu'imprévisibles car ils risquent d'endommager sévèrement les systèmes d'information si des mesures de protection ne sont pas prises au préalable. Non seulement de grandes pertes de données seront causées et porteront atteinte aux exigences de sécurité et de confidentialité, mais aussi de considérables pertes de chiffre d'affaires pourront s'installer très rapidement et durablement. Certaines entreprises ne peuvent pas se remettre des pertes financières causées par les sinistres, d'où l'importance, voire l'impérativité, d'éviter l'occurrence de ces sinistres. L'une des approches adoptées dans cet élan anticipatif est la prévention par prévision des risques pouvant être à l'origine de ces défaillances.

Compte tenu de ses connaissances, chaque entreprise doit consacrer ses ressources pour assurer la continuité de son exercice en dépit de la présence de toutes sortes de turbulences potentielles. Dans le cadre de ce processus, il est important de développer une compréhension du large éventail des menaces auxquelles une entreprise peut être confrontée, dans le but d'avoir des réponses planifiées et testées pouvant assurer à l'entreprise une sortie saine de la crise qu'elle aura subit.

L'ensemble de ces procédures conçues pour protéger l'infrastructure et le système d'information de l'entreprise est appelé ***Plan de Reprise d'Activité*** (PRA) ou ***Disaster Recovery Plan*** (DRP).

Ce mémoire va présenter un cas d'étude de plan de reprise d'activité. Il est composé de 3 chapitres.

Dans le *premier chapitre*, nous revenons sur la définition d'un plan de reprise d'activité, notamment en présentant les éléments qui le composent, comment se fait une étude de risque, et quelles sont les stratégies qui peuvent nous aider à élaborer un PRA adapté à une entreprise quelconque.

Dans le *deuxième chapitre*, nous avons présenté une architecture de sauvegarde d'une entreprise Algérienne, et avons proposé des améliorations dans le but d'atteindre de meilleurs objectifs en termes de temps de sauvegardes et de récupération des données.

Dans le *troisième chapitre*, nous avons simulé un scénario de récupération de données, à l'aide d'un logiciel open source de reprise d'activité après sinistre.

Nous finirons de manière classique par conclure nos travaux et leur proposer des perspectives.

CHAPITRE I Terminologie, caractéristiques et état de l'art d'un plan de reprise d'activité (PRA)

I.1. Introduction

I.2. Définition

I.3. Cycle de vie d'un PRA

I.4. Périmètre d'un PRA

I.5. Étude de risques

I.5.1. Étapes d'une étude de risque

I.6. Stratégies du PRA

I.6.1. Sauvegardes

I.6.2. Utilisation d'un site externe de reprise

I.6.3. Stratégie basée sur le Cloud

I.6.4. Stratégie basée sur le DRaaS (PRA as a Service)

I.7. Conclusion

CHAPITRE I : État de l'art d'un plan de reprise d'activité

I.1. Introduction

Le monde de l'entreprise requiert un certain nombre de ressources technologiques et humaines assurant la continuité de sa productivité. Des désastres peuvent arriver et entraver le bon fonctionnement de l'entreprise en ayant un impact sur ses ressources, ce qui peut conduire à l'interruption de son activité et par conséquent à la baisse de son chiffre d'affaires.

Les plans de reprises d'activité après sinistre se concentrent sur l'analyse des désastres qui représentent une menace pour le système d'information de l'entreprise, et sur l'élaboration des différentes stratégies et solutions qui vont permettre à l'entreprise de reprendre ses fonctions et activités le plus rapidement possible.

I.2. Définition

Un plan de reprise d'activité (PRA) représente un ensemble de mesures et procédures définies en état « nominal » en prévision d'une situation de « désastre » susceptible d'affecter négativement le système d'information d'une entreprise et entraîner une perte d'autorité de la marque, une perte de confiance des clients et une perte financière. Le PRA a pour but d'atténuer les effets dévastateurs de la catastrophe. Cela étant, il garantira :

- La limitation des pertes de données.
- Réduction des pertes financières.
- Une reprise rapide de l'activité (des systèmes informatiques).

Un PRA n'est pas uniquement conçu pour répondre à tout incident important qui peut se produire, mais aussi pour conforter l'image de fiabilité de l'entreprise auprès de ses clients et partenaires. [1] [2]

I.3. Cycle de vie d'un PRA

La mise en œuvre d'un PRA suit une séquence logique d'étapes de façon progressive et continue, l'ensemble de ces étapes est appelé « ***cycle de vie*** » d'un PRA (***Figure I.1***).

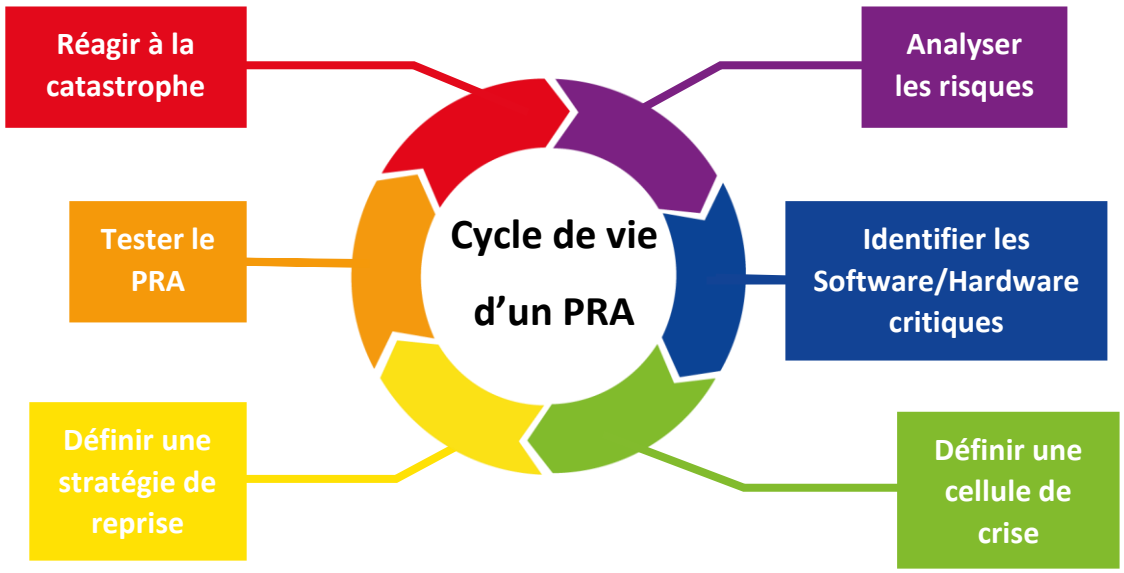


Figure I.1 : Cycle de vie

La quantité de suivi et d'investissement d'un PRA peut différer d'une entreprise à une autre et donc les étapes du cycle de vie d'un PRA peuvent être développées ou étendues selon les besoins particuliers de chaque organisation.

Chaque étape du cycle de vie d'un PRA est une phase importante qui dépend et fait usage des autres phases.

- **Analyser l'impact des différents sinistres susceptibles de se produire.**
- **Identifier les fonctions/activités et technologies essentielles à la poursuite des activités de l'entreprise.**
- **Définir une cellule de crise :** nombre de personnes intervenant dans l'exécution du PRA, chacune ayant un rôle précis à jouer en cas de désastre. Une cellule de crise est essentiellement composée de membres permanents : directeurs et auteurs du PRA, et d'autres mobilisables : responsables des différents services et personnel, qui seront appelés à participer à cette cellule si des décisions qui concernent leurs services sont à prendre.

- **Définir la stratégie de reprise d'activité la mieux adaptée à l'entreprise.**
- **Réaliser un test du PRA établi :** étape qui doit être répétée au minimum une fois par an car les ressources humaines et matérielles d'une entreprise peuvent changer, son but est de limiter tout risque de défaillance du PRA en cas de catastrophe.
- **Réagir au moment où le sinistre se produit :**
  - Evaluer le degré de dommages causés et décider s'il y a besoin d'exécuter le PRA.
  - En cas d'impact majeur, la cellule de crise doit être notifiée et informée de la catastrophe, le plan de reprise d'activité est mis à exécution.

I.4. Étude de risque

Le processus d'étude de risques permet d'identifier et de documenter les risques liés à l'entreprise, cette étude a pour but d'envisager le pire scénario, tel que : désastres naturels, techniques ou humains, et la manière dont une catastrophe pourrait affecter l'activité de l'entreprise. Elle est, à ce titre, une étape cruciale dans la perspective d'un PRA.

I.4.1. Étapes d'une étude de risque

L'identification, l'évaluation, le traitement, le suivi et le rapport des risques sont les 4 étapes qu'il faut suivre pour faire une étude de risque (***Figure I.2***)

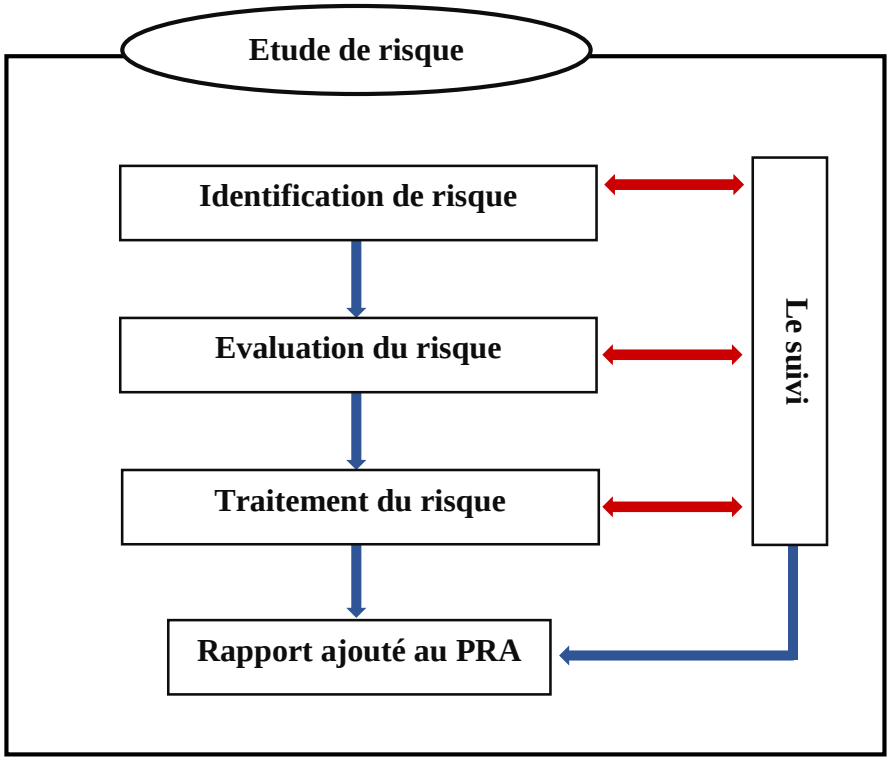


Figure I.2 : Processus d'étude de risques

- **Identification des risques :** Il s'agit de rédiger une liste exhaustive de tous les risques auxquels l'entreprise est exposée. Ici nous avons listé les risques auxquels peut être soumise une entreprise en Algérie (***Figure I.3***) [3] [4]

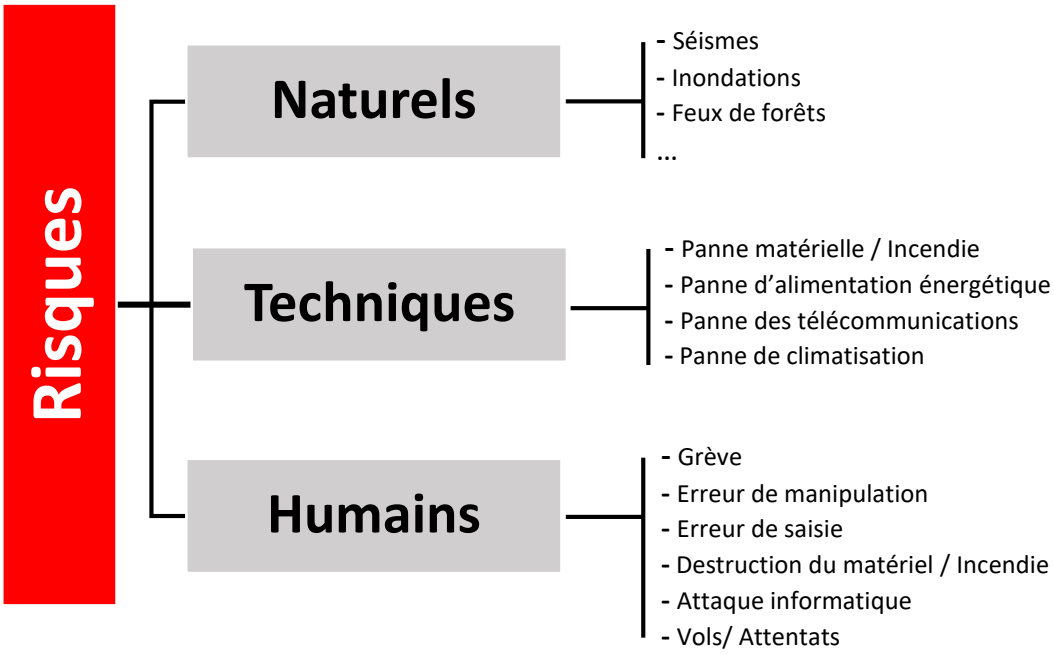


Figure I.3 : Liste de risques identifiés en Algérie

- **Évaluation des risques :** Ces risques sont ensuite classés par ordre d'importance en fonction de leur complexité et de leur impact sur l'entreprise. Il existe deux types d'évaluation des risques : *qualitative* et *quantitative*, et les deux types sont nécessaires pour une évaluation complète.

  - **Évaluation qualitative :** elle cible particulièrement la gravité de l'impact et la probabilité d'occurrence d'un évènement.

    Évaluation de la gravité des impacts des risques : elle définit quel impact peut avoir une catastrophe sur l'entreprise. Elle est représentée sur une échelle, et souvent classée en 5 niveaux : *négligeable*, *bas*, *modéré*, *critique* ou *catastrophique* (***Tableau I.1***).

	Niveaux d'impact	Signification
1	Négligeable	Pas d'impact significatif
2	Bas	Le risque a un impact sur l'entreprise, mais il est atténué par des mesures efficaces.
3	Modéré	Le risque a un impact significatif et n'a pas encore été atténué par les mesures. Il peut être géré en dehors du PRA.
4	Critique	Le risque a un impact significatif sur un ou plusieurs aspects. Il doit être traité au sein du PRA.
5	Catastrophique	Le risque a un impact *majeur* sur un ou plusieurs aspects. Il doit être *prioritairement* traité au sein du PRA.

Tableau I.1: Niveaux d'impact

Évaluation de la probabilité d'occurrence des risques : elle définit la probabilité qu'un évènement se produise ou non. Elle est représentée sur une échelle de 5 niveaux également : *improbable*, *rare*, *occasionnel*, *probable* ou *fréquent* (***Tableau I.2***)

	Niveaux de probabilité	Signification
1	Improbable	Ne se produit presque jamais.
2	Rare	Se produit moins d'une fois par an.
3	Occasionnel	Se produit environ 2 à 3 fois par an.
4	Probable	Se produit environ 3 à 4 fois par an.
5	Fréquent	Peut se produire environ 5 fois et plus par an.

Tableau I.2: Niveaux de probabilité

Un tableau d'évaluation qualitative est le résultat d'une fusion des deux tableaux précédents, il est représenté avec une matrice (5x5), dans l'axe des ordonnées on trouve les niveaux d'impact cités dans le ***Tableau I.1***, en abscisse les niveaux de probabilité cités dans le ***Tableau I.2***, le croisement des deux axes de la matrice donne des niveaux de risque gradués de 1 à 5, en fonction du couple (Impact x Probabilité), représentés dans le ***Tableau I.3***.

Niveaux d'impact		**Niveaux de probabilité**				
		Improbable **1**	Rare **2**	Occasionnel **3**	Probable **4**	Fréquent **5**
	Négligeable **1**	**1**	**1**	**1**	**1**	**1**
	Bas **2**	**1**	**1**	**2**	**2**	**2**
	Modéré **3**	**2**	**2**	**2**	**3**	**4**
	Critique **4**	**2**	**3**	**4**	**4**	**5**
	Catastrophique **5**	**2**	**3**	**5**	**5**	**5**

Tableau I.3: Evaluation qualitative

En se basant sur les tableaux précédents, il est possible maintenant d'attribuer une valeur de 1 à 5 (niveau de risque) pour chaque source de risque citée dans l'étape d'identification (***Tableau I.4***).

Risques	*Description*	*Niveau de risque*
Incendie	Acte prémédité, installation électrique non conforme, mal entretenue ou surexploitée.	3
Dégâts des eaux	Fuite de plomberie, infiltration d'eau pluviale.	2
Explosion	Présence d'un combustible…	2
Risques Naturels		
Séismes	Zone à risque	3
Inondations	Pluie torrentielle, débordement indirect d'une réserve d'eau (de surface ou souterraine) …	4
Risques Techniques		
Panne matérielle	Usure, défaut de maintenance, mauvais emploi	3
Panne d'alimentation énergétique	Coupures, panne chez fournisseur d'électricité	3
Panne des télécommunications	Panne de réseau téléphonique	3
Panne de climatisation	Surchauffe de matériel	3
Risques Humains		
Grève	Mouvement social	2
Erreur de manipulation	Mauvaise utilisation du matériel/logiciel	3
Erreur de saisie	Données entrées erronées …	3
Vol / Destruction du matériel	Sabotage des équipements, émeutes…	2
Attaque informatique	Espionnage, virus…	3

Tableau I.4: Risques classés selon une évaluation qualitative

- **Evaluation quantitative :** elle analyse l'impact financier sur l'entreprise. Elle est représentée sur une échelle de 3 niveaux : *moyen*, *élevé* ou *critique*.

Lors de l'évaluation de risques précédente, les scénarios de crise retenus en pratique sont ceux qui ont une valeur estimée dans le ***Tableau I.4*** supérieure ou égale à ***3*** et un impact financier ***moyen***, ***élevé*** ou ***critique***.

- **Traitement des risques :** Les risques peuvent faire l'objet d'un plan de traitement et, surtout, ils permettent à une entreprise d'établir sa stratégie d'intervention. Le plan de traitement des risques a pour objectif de réduire la probabilité que le risque se concrétise ou de diminuer son incidence.

  Le traitement du risque peut inclure les actions suivantes : Accepter, Réduire, Transférer et Eliminer le risque. [5] [6]

  - **Accepter le risque :** Cela se produit lorsque l'entreprise reconnaît que la perte potentielle causée par un risque n'est pas considérable, donc elle choisit de ne pas le tenir en compte, de le tolérer.
  - **Réduire le risque :** Minimiser les effets des accidents avec des actions en protection. Par exemple : si on veut réduire le risque de fuite de liquide d'un centre de données, il est possible d'engager un spécialiste en étanchéité pour mettre en place une enduction d'un produit à base de caoutchouc ou faire appel un spécialiste en bâtiment pour installer des systèmes conçus à détourner l'eau de l'installation du centre. [7]
  - **Transférer le risque :** Les répercussions négatives des risques et de leur responsabilité peuvent être transférées à un tiers qui est jugé plus apte à en assurer le traitement (habituellement effectué avec une assurance). Par contre, le transfert de risque n'élimine pas le risque.
  - **Eliminer le risque :** Certains les risques recensés sont le résultat d'une méconnaissance de la situation ou manque de matériel ... etc. Ainsi il est parfois possible de les éliminer en menant des enquêtes plus poussées, par exemple : un incendie peut arriver suite à un court-circuit d'un composant d'un câble défectueux. Un moyen d'éliminer ce risque serait de vérifier constamment l'état des câbles.

- **Le suivi et le rapport d'un risque :** Le suivi est un processus essentiel pour mener à bien un projet et y contribuer. Il est utilisé pour évaluer l'état d'avancement d'une étude de risque.

  Les rapports des risques sont un processus de communication des données sur les risques et le rendement aux parties prenantes en temps réel.

En se basant sur les résultats de l'étude de risque, les responsables et administrateurs informatiques pourront identifier les mesures qui peuvent aider à réduire les menaces ou à atténuer leur gravité si elles se produisent. Ces analyses peuvent ensuite être traduites en valeurs RPO et RTO (définies et détaillées dans le titre suivant) et doivent être examinées et approuvées par les différents responsables des services ainsi que le directeur général.

I.5. Périmètre d'un PRA

Un périmètre représente le cercle fonctionnel de l'entreprise, il doit identifier tout ce qui peut guider ses choix stratégiques relatifs au PRA.

Il est caractérisé par deux étapes. La première étape représente le champ d'action du PRA. Elle délimite les actifs critiques (services, activités et applications) de l'entreprise qu'il faut maintenir démarrés en cas de sinistre. Pour ce faire, il faudra d'abord identifier toutes les fonctions et activités réalisées par le personnel. Ensuite ces activités doivent être classées par ordre d'importance et de criticité (ceci requiert la participation des différents responsables des services de l'entreprise).

La deuxième étape consiste à définir les objectifs RTO et RPO (***Figure I.4***) [8]

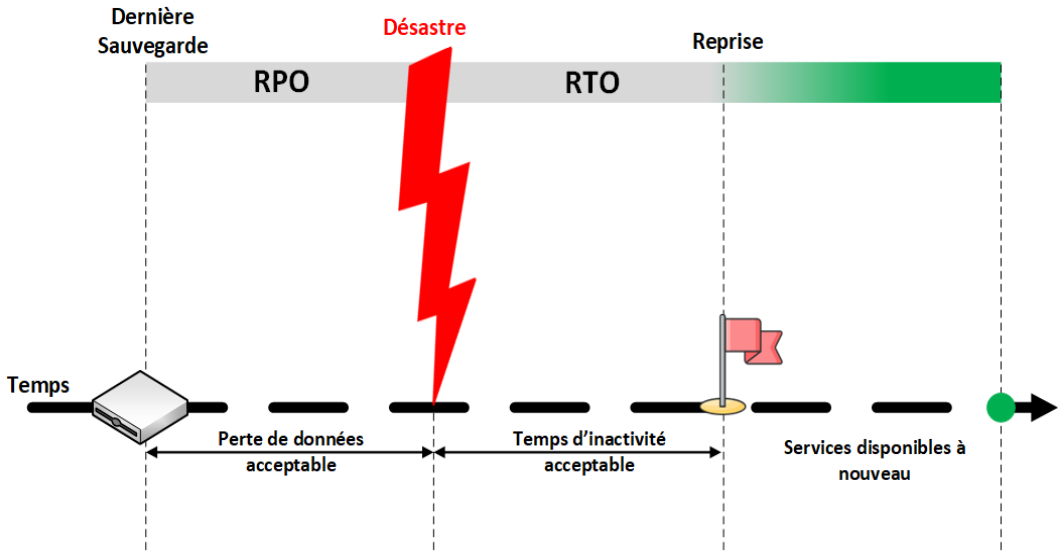


Figure I.4 : Position du RTO/RPO pendant un sinistre [8]

La ***Durée Maximale d'Interruption Admissible*** (DMIA) également connue sous le nom de ***Recovery Time Objective*** (RTO) représente la durée d'interruption d'activité

maximale admissible pendant laquelle une application peut être indisponible sans causer de dommages importants à l'entreprise. Cette durée correspond à l'intervalle de temps maximum entre le moment de la notification de l'incident et la reprise normale du service. Pour définir le RTO, il faut tenir compte du coût par heure d'indisponibilité et des budgets et ressources disponibles.

La ***Perte de Données Maximale Admissible*** (PDMA) également connue sous le nom de ***Recovery Point Objective*** (RPO) représente l'intervalle de temps correspondant à la quantité maximale de données perdue acceptable par l'entreprise. En d'autres termes, le RPO détermine ce qui est considéré comme étant une perte de données acceptable entre le dernier point de sauvegarde et l'interruption du service. Pour définir le RTO, il faut tenir compte du coût des données et des budgets et ressources disponibles.

Par exemple : Une entreprise a défini un RPO de 24h. L'un de ses serveurs tombe en panne à 8h. On va restaurer la dernière sauvegarde qui a été effectuée à 20h la veille de la panne. La fraîcheur des données sera donc de 12h, l'objectif RPO est vérifié. [8]

I.6. Sauvegardes

Définir une stratégie de sauvegarde est essentiel pour réaliser un PRA, car une perte de données est une catastrophe susceptible d'entraîner des conséquences encore plus désastreuses si les données ne sont pas restaurées dans un délai raisonnable et admissible.

Pour choisir une bonne stratégie de sauvegarde, il faut prendre en considération les points suivants :

- La sauvegarde dépend principalement des objectifs RTO et RPO. La fréquence de sauvegarde va être définie en fonction de la valeur du RPO fixée lors de la définition du périmètre du PRA. Le processus de récupération de données ne doit pas dépasser la valeur du RTO.
- Le mécanisme de compression et de déduplication de sauvegarde (détecter la répétition des données et ne stocker les mêmes données qu'une seule fois) optimise l'espace de stockage des sauvegardes et le débit nécessaire aux transferts de ces données.
- Avant d'effectuer une sauvegarde / récupération, il est important de définir quelles sont les données les plus critiques à sauvegarder / récupérer, et quelle est la granularité

souhaitée pour chaque donnée (faut-il sauvegarder / récupérer toute la donnée ou juste une partie).

- Une sauvegarde de données peut être effectuée sur un support physique (réalisée au niveau des médias de stockage dans le site principal de l'entreprise ou même dans un site secondaire), comme elle peut être effectuée dans le Cloud.

I.7. Stratégies du PRA

La reprise après sinistre est un élément essentiel de la protection des données et du maintien de la continuité des activités.

Cependant, avec autant d'options différentes de planification de reprise après sinistre qu'une entreprise peut mettre en œuvre, le processus de recherche de la meilleure stratégie peut être écrasant. Chaque entreprise est différente, et donc chaque PRA est à adapter selon l'entreprise et ses spécificités, il n'y a pas de modèle idéal.

I.7.1. Utilisation d'un site de reprise

Cette solution est la plus onéreuse puisqu'il s'agit de sélectionner un site secondaire, incluant les éléments matériels essentiels à la reprise d'activité de l'entreprise (serveurs, baies de stockage…), prêt à l'emploi si un sinistre a lieu au niveau du premier site et que ce dernier n'est plus fonctionnel. Elle est souvent adoptée par les très grandes entreprises ayant des besoins importants en information et des objectifs de temps de récupération strictes. Il existe deux options du site de reprise : ***interne*** et ***externe***. Une entreprise met en place et gère un site interne, tandis qu'un site externe est détenu et exploité par un fournisseur externe. [9]

Lors du choix d'un site de reprise, l'entreprise doit prendre en compte les facteurs suivants :

- **Emplacement** : il est important de définir à quel endroit et distance se trouve le site de reprise. Un site de reprise plus rapproché du site principal favorise la synchronisation et facilite la gestion du personnel.
- **Ressources** : définir quelles ressources et technologies de l'entreprise sont essentielles à l'entreprise pour poursuivre ses activités.

- **Coût** : une entreprise doit savoir quel montant elle pourrait dépenser pour un site de reprise adéquat. Plus il y a de ressources (matérielles, logicielles et humaines) sur le site plus le coût est élevé.

I.7.2. Stratégie basée sur le Cloud (Cloud DR)

Cette approche du PRA est mieux adaptée aux petites entreprises sur le plan financier, puisqu'il est possible d'utiliser le centre de données du Cloud comme site de sauvegarde et de récupération de données, d'applications et d'autres ressources, plutôt que de s'investir davantage dans de nouvelles installations et systèmes.

L'utilisation des ressources en Cloud permet une meilleure maîtrise des coûts et un accès à distance en cas de désastre.

La différence principale entre le PRA dans le Cloud et la reprise dans un site réside dans l'effort de mise en place et de maintenance du matériel et des logiciels requis pour la sauvegarde et la récupération. Les entreprises qui choisissent d'élaborer un PRA basé sur le Cloud bénéficient d'un grand avantage car toutes les technologies sont externalisées et ne devraient pas être mises en place et gérées dans des locaux propres. [10]

I.7.3. Stratégie basée sur le DRaaS (PRA as a Service)

Il s'agit de services industrialisés par des prestataires qui proposent une plateforme prête à l'emploi qui automatise les tâches de sauvegarde, de récupération et de reprise d'activité.

Dans un modèle DRaaS, les serveurs physiques ou les machines virtuelles d'une organisation sont répliqués vers un fournisseur de services tiers. Le fournisseur de services héberge l'infrastructure du client, en utilisant des ressources Cloud publiques ou privées, fournissant une cible de basculement en cas de sinistre. [11]. Le DRaaS peut étirer le budget en éliminant les investissements que les entreprises peuvent faire pour maintenir leurs propres espaces de reprise après sinistre hors site.

I.8. Bibliographie des architectures

Un de nos objectifs originels était de retrouver un cas de figure concret sur lequel on peut appliquer un PRA. L'approche la plus naturelle était donc de chercher un stage auprès d'une entreprise nationale dans le domaine informatique et communications

pouvant nous permettre de réaliser une telle étude. A cet effet, nous nous sommes rapprochées de « Algérie Télécom », « Ooredoo », « Djezzy », « Mobilis », « Huawei » de par le fait de leur position en tant que leaders dans le domaine du réseau. Malheureusement pour nous et en dépit de tous les efforts fournis, nos tentatives étaient vaines. Devant cette contrainte, nous étions obligées de simuler une architecture conceptuelle d'un centre de données sur laquelle on pourrait élaborer et implémenter un PRA.

Ceci nous a amené à faire une recherche bibliographique qui nous a permis de faire le tour des architectures existantes, d'établir des études comparatives de ces architectures et d'improviser un type sur la base de cette recherche documentaire. Concrètement, ce travail est synthétisé dans les paragraphes suivants.

I.8.1. Etude comparative de topologies réseaux des centre de données

Pendant de nombreuses années, les centres de données ont été construits sur une architecture à trois niveaux. Au fil du temps, la topologie dite « Leaf Spine » est devenue la principale mise en œuvre du réseau des centres de données en raison de sa fiabilité, de son évolutivité et de ses performances. [12]

- **Architecture Leaf-Spine 2-Tiers**

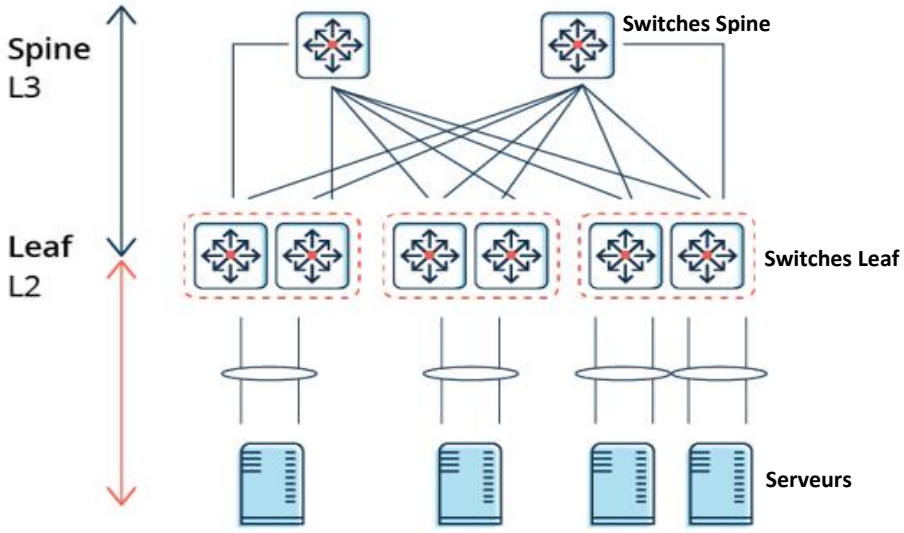


Figure I.5 : Topologie Leaf Spine

- Topologie réseau hiérarchique à 2 niveaux (Leaf, Spine) (***Figure I.5***) [13]

  Couche Leaf : (feuilles) commutateurs d'accès qui se connectent aux serveurs.

  Couche Spine : Le cœur du réseau, s'occupe de l'interconnexion entre les feuilles.

  Topologie à maillage complet : chaque commutateur Leaf se connecte à chaque commutateur Spine.

- Architecture moderne de plus en plus utilisée, du moment que plus de 70% du trafic de données dans un Datacenter est un trafic Est-Ouest (de serveur en serveur) alors, un flux de trafic optimisé et à faible latence est impératif.

- Cette architecture garantit que le trafic contient le même nombre de sauts vers sa prochaine destination ce qui va assurer une latence faible.

- Le Leaf-Spine devient progressivement l'architecture dominante.

- Le protocole STP est éliminé et le routage se fait de façon à ce que chemin emprunté soit choisi au hasard pour que la charge du trafic soit répartie équitablement entre les commutateurs supérieurs.
- **Evolutivité :** Si un lien est invité à gérer plus de trafic qu'il ne le peut à tout moment, il suffit d'ajouter un nouveau commutateur Spine, le connecter à chaque commutateur Leaf et le problème est résolu.

- **Architecture traditionnelle 3-Tiers**

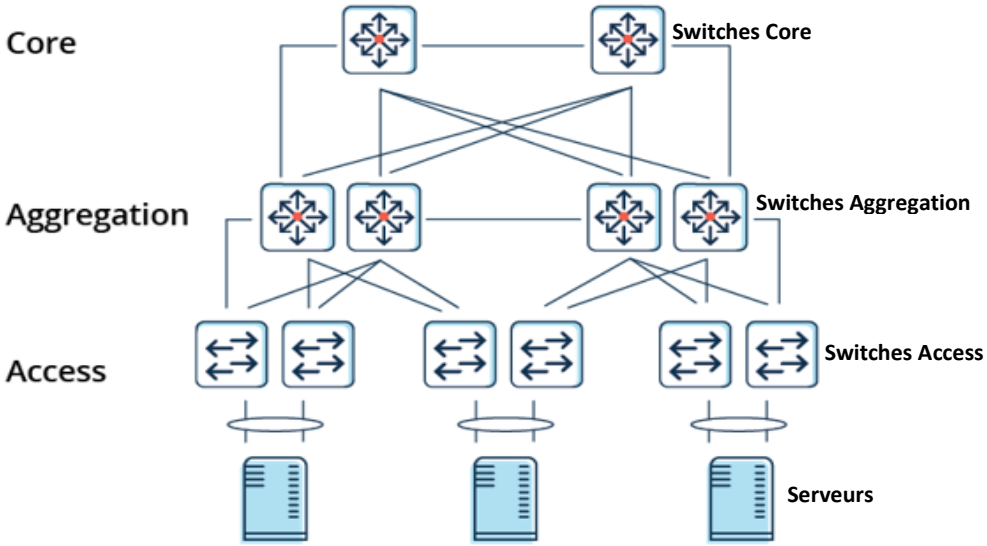


Figure I.6 : Topologie Traditionnelle

- Architecture hiérarchique à 3 niveaux (Acces, Aggregation, Core) (***Figure I.6***) [13]

  Couche accès : commutateurs connectés aux serveurs appelés Switch *ToR* (Top of Rack).

  Couche agrégation : commutateurs de distribution qui se connectent aux commutateurs d'accès, couche fournissant d'autres services tels que le pare-feu + ***IPS*** (système de contrôle qui rejette les paquets représentants une menace) + ***IDS*** (Système de détection d'intrusion qui analyse et surveille le trafic réseau).

  Couche core : ou centrale, assure la connectivité entre les commutateurs d'agrégation et le transfert des paquets entrant et sortant du Datacenter (trafic Nord-Sud).

- Première architecture conçue particulièrement pour un trafic Nord-Sud (Serveur-client).

- Le trafic entre les différents commutateurs d'accès doit être transmis via des niveaux de commutation de niveau supérieur selon un schéma nord-sud également, ce qui ajoute des possibilités de perte de paquets et de latence importante créées par des connexions supplémentaires entre les commutateurs → problèmes dans les entreprises avec un flux important de données.
- Ce type d'architecture peut être utilisé dans les centres de données les plus petits où la latence n'est pas un facteur très important.
- Entre les deux couches accès et agrégation, une configuration correcte du protocole STP est nécessaire car en cas de défaillance de ce protocole des boucles continues peuvent être provoquées.
- **Evolutivité :** Si un lien est invité à gérer plus de trafic qu'il ne le peut à tout moment, cela est normalement corrigé en ajoutant des liens ou des commutateurs supplémentaires pour faire face au trafic excédentaire. Parfois, cela est difficile et nécessite certainement une reconfiguration du réseau et des temps d'arrêt.

I.8.2. Architectures et topologies proposées

La topologie Leaf Spine à son tour est divisée en deux sous-types de topologies présentées ci-dessous (***Figure I.7***) (***Figure I.8***) [14]

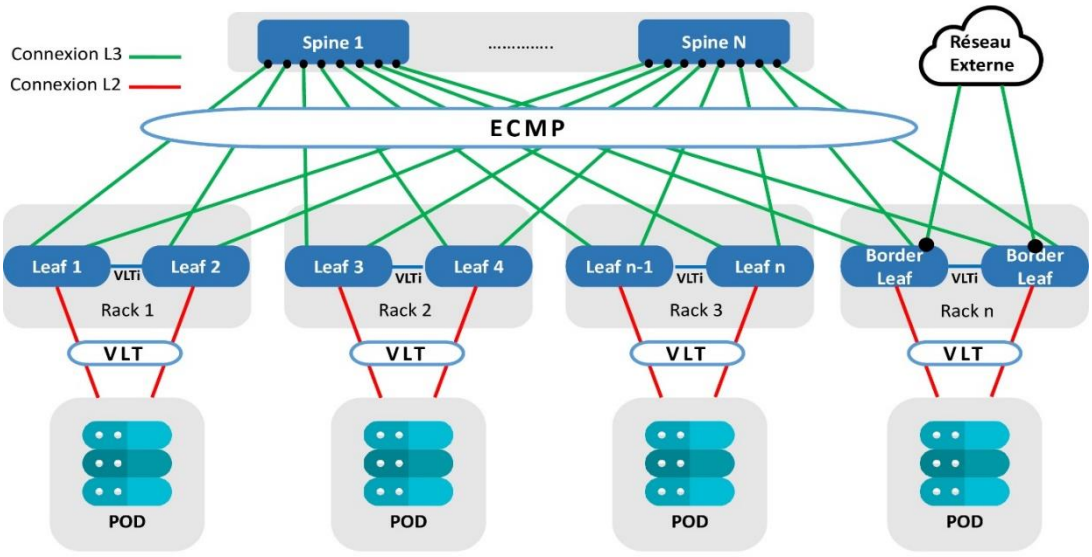


Figure I.7 : Layer 3 Leaf-Spine 2-Tiers Topologie : Centre de Données

- Le trafic entre les switches Leaf et Spine est routé.
- La limite entre la couche 2 / couche 3 se trouve au niveau du switch Leaf.

- Dans la topologie Leaf-Spine layer 3, les switches Spine ne sont jamais connectés les uns aux autres.
- Le protocole ECMP est utilisé pour répartir équitablement le trafic entre les différents équipements du réseau.
- Les connexions entre les POD et les switches Leaf se font selon une topologie L2 (Layer 2).
- La connexion aux réseaux externes se fait à partir d'une paire de switches Leaf qui se trouvent sur les bordures de l'architecture.
- Dans une topologie L3, il peut y avoir jusqu'à 4094 Vlan par switch rack.
- En cas d'utilisations de Cloud ou de Virtualisation, la topologie Layer 3 est recommandée.
- Une topologie layer 3 est scalable et mieux adapté aux grandes infrastructures réseau (possibilité d'ajouter autant de Spine Switch que nécessaire).

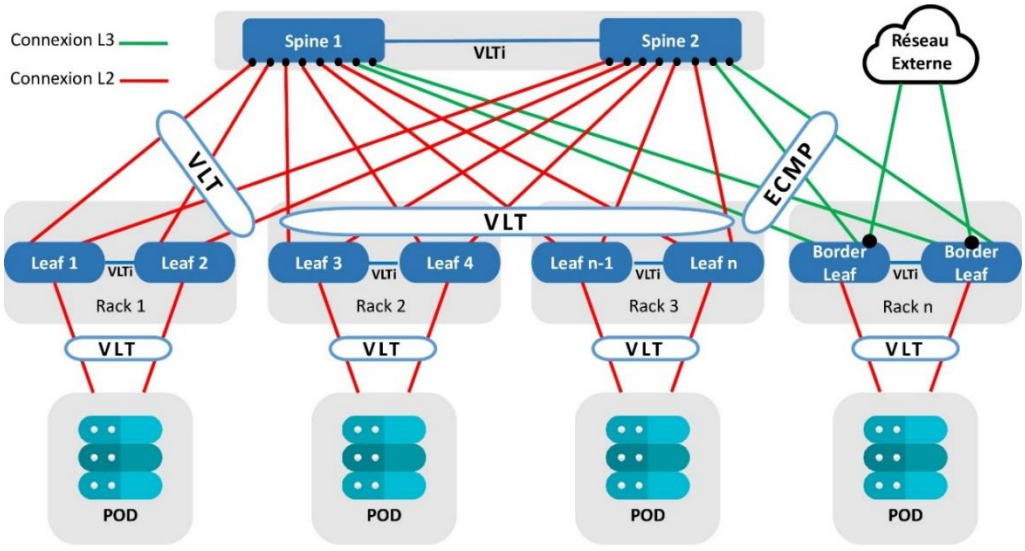


Figure I.8 : Layer 2 Leaf-Spine 2-Tiers Topologie : Centre de reprise

- Le trafic entre les switches Leaf et Spine est commuté excepté pour les switches qui se trouvent aux extrémités.

- Le protocole VLT est utilisé pour répartir le trafic entre les différents switches Leaf-Spine à l'exception des switches qui se trouvent à l'extrémité.
- Les connexions entre les POD et les switches Leaf se font selon une topologie L2 (Layer 2).
- La connexion aux réseaux externes se fait à partir d'une paire de switches Leaf qui se trouvent sur les bordures de l'architecture.
- Le protocole ECMP est utilisé uniquement au niveau des connections L3 entre Switches Spine et Leaf se trouvant sur les bordures de l'architecture.
- Une topologie L2 est généralement moins complexe qu'une topologie L3.
- Une topologie L2 est limitée à 4094 Vlan dans un switch ***fabric***.
- Le nombre de Switch Spine est limité à 2 dans une topologie L2.
- **VLT (Virtual link trunking)** : Est un protocole d'agrégation layer 2 qui permet un partage d'information entre 2 nœuds (switches et équipements).
- **ECMP (Equal-cost multi-path routing)** : Est une stratégie de routage réseau qui permet au trafic d'un même flux, ayant la même source et la même destination, d'être transmis par plusieurs chemins de coût égal.
- **Switch fabric :** Topologie de nœuds interconnectés par des switches.

Selon ces deux topologies, nous avons proposé deux architectures : Celle d'un centre de données correspondant à la topologie Layer 3 Leaf-Spine (***Figure I.9***), et celle d'un centre de reprise correspondant à la topologie Layer 2 Leaf-Spine (***Figure I.10***).

Les deux architectures sont composées de serveurs (WEB, FTP, Mail) connectés à des switches DMZ et des parefeux afin de renforcer la sécurité du réseau, ainsi que de serveurs virtuels (ESX), plus un serveur NAS de stockage en réseau présent uniquement sur la première architecture (Centre de données). Les switches multi-layers L3 servent à connecter les différentes composantes des architectures.

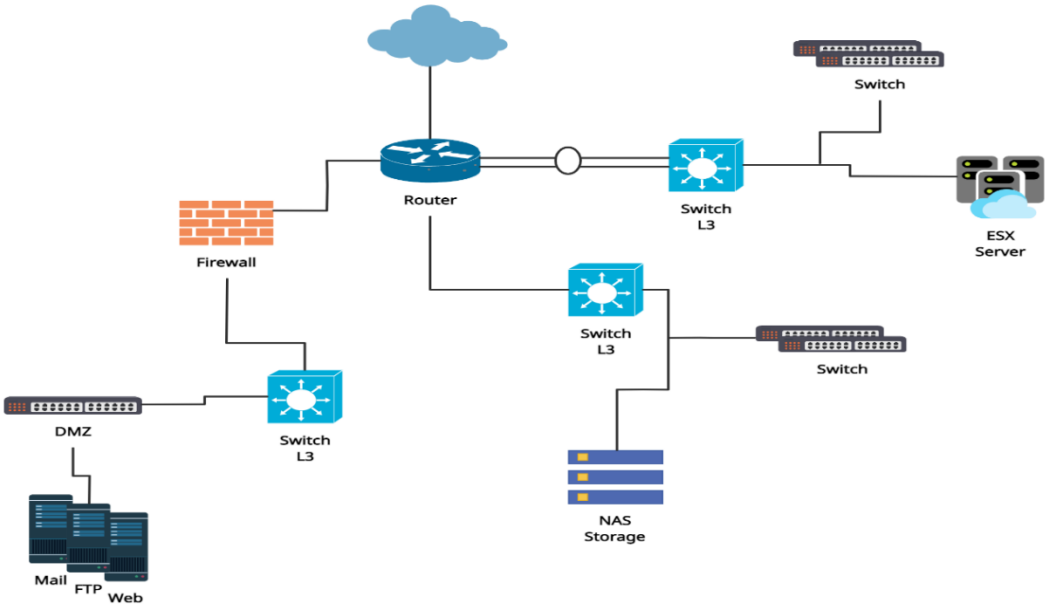


Figure I.9 : Architecture proposée du centre de données

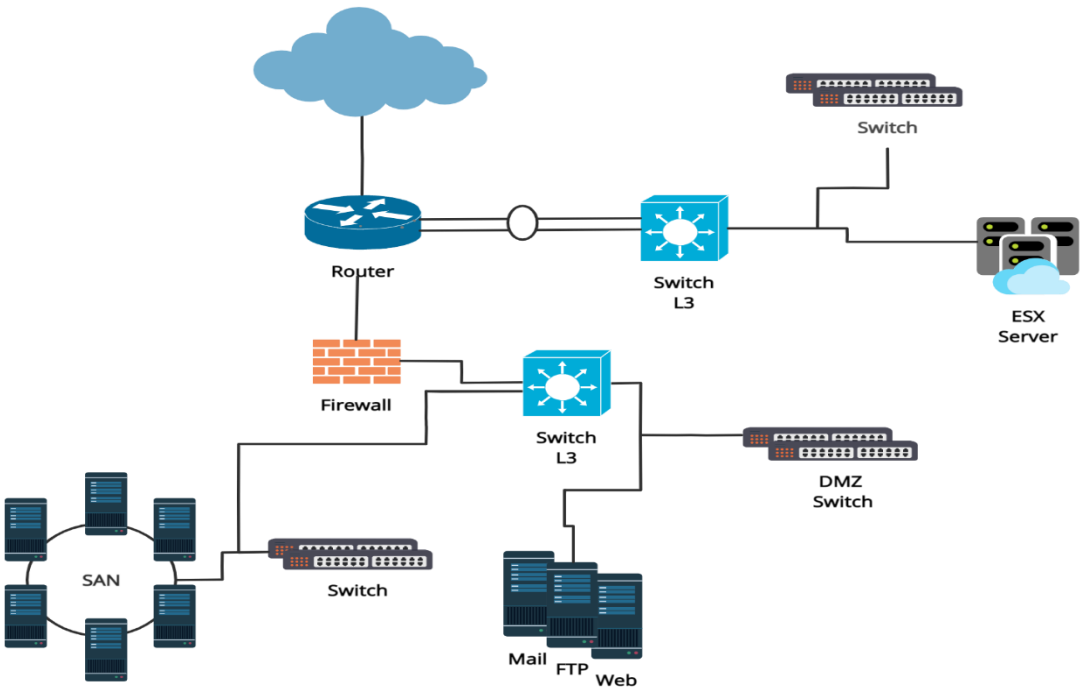


Figure I.10 : Architecture proposée du centre de reprise

Le manque de données concrètes et pragmatiques a créé une ambiguïté et nous a obligé de reformuler à plusieurs reprises nos objectifs et perspectives pour l'élaboration d'un PRA. Il a fallu donc revenir vers la recherche de données concrètes auprès d'une entreprise en vue de sortir de ce joug.

Heureusement, la solution à ce problème a été trouvée grâce à la rencontre avec un représentant de l'équipe iServ Solutions (iSS). Il s'agit de fournisseurs et prestataires de services et solutions informatiques. L'entreprise est spécialisée dans le domaine de protections de données, réseaux et sécurité, reprise d'activité après désastre ainsi que d'autres services. Elle compte jusqu'à 50 employés et a son siège à Alger.

Cette entreprise nous a proposé un modèle d'architecture réel d'une entreprise cliente (néanmoins anonyme), ce qui nous a permis de réajuster notre perspective en termes de PRA.

Ce modèle d'architecture a été adopté dans notre étude et a été exhaustivement traité au chapitre 2.

I.9. Conclusion

Chaque entreprise est responsable de la disponibilité et de l'intégrité de ses activités et ses services. Il est donc important d'identifier et de définir ce qu'est un risque et d'élaborer le plan de reprise d'activité qui correspond le mieux à cette définition, en déterminant quels sont les désastres qui peuvent nuire à l'activité de l'entreprise, quels services et applications font partie du périmètre, et quelles sont les stratégies les mieux adaptées à l'entreprise qu'il faut suivre pour assurer sa reprise d'activité.

CHAPITRE II Optimisation d'objectifs de reprise

II.1. Introduction

II.2. Architecture initiale de l'entreprise « X »

II.2.1. Composantes de l'architecture

II.2.2. Contraintes et limitations de l'architecture

II.3. Architecture optimisée

II.4. Conclusion

CHAPITRE II Optimisation d'objectifs de reprise

II.1. Introduction

Ce travail a pour but d'améliorer l'une des stratégies du PRA ; atteindre de meilleurs objectifs concernant le temps de sauvegarde / récupération des données critiques d'une entreprise, et par conséquent valider les objectifs RTO et RPO.

Nous avons travaillé avec une entreprise réelle qui nous a proposé son modèle initial d'architecture de sauvegarde. Pour des besoins de confidentialité et afin de donner une forme d'anonymat à l'entreprise nous lui avons attribué « X » comme nom.

II.2. Architecture initiale de l'entreprise « X »

L'architecture existante de sauvegarde est située dans le site de l'entreprise « X » sous un environnement Symantec Netbackup 7.5. Elle comporte un certain nombre de serveurs avec des fonctionnalités différentes : clients standards, deux Clusters : 2 serveurs en Cluster Oracle, 2 serveurs en Cluster Veritas, connectés à 2 switches SAN qui à leur tour sont connectés à une baie de stockage, ainsi qu'un Master/Média serveur connecté à une Tape Library, le tout interconnecté via un switch de sauvegarde 1 Go (***Figure II.1***).

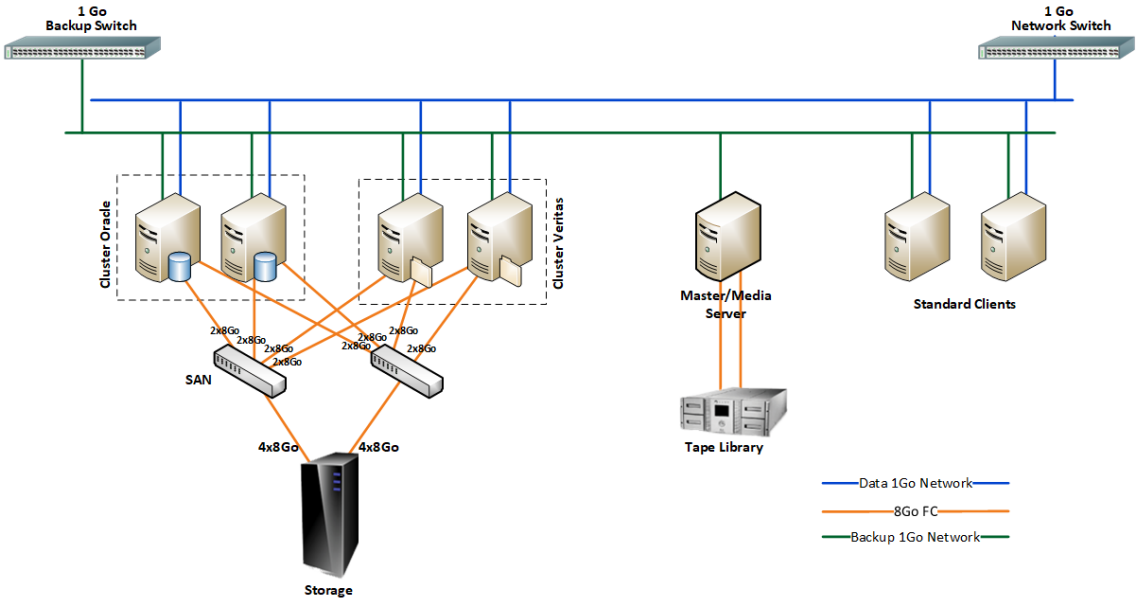


Figure II.1 : Architecture de l'entreprise X

II.2.1. Composantes de l'architecture

L'architecture initiale de l'entreprise « X » est constitué des éléments présents dans la (***Figure II.1***) définis ci-dessous :

- **NetBackup (NBU)** : Est une solution logicielle hétérogène (multiplateforme) client-serveur conçue pour les clients de l'entreprise. La fonctionnalité de base du logiciel comprend la sauvegarde, la récupération, l'archivage et la reprise après sinistre.
- **Master Server** : Représente le serveur principal « cerveau » dans un environnement NBU. Il sert à contrôler, planifier, suivre les activités de sauvegarde et de reprise, à gérer les médias de stockage et le catalogue NBU (fichiers contenant les informations vitales des sauvegardes effectuées et planifiées). Ce serveur peut également être configuré comme un serveur multimédia.
- **Media Server** : Ce serveur gère la lecture, l'écriture et le mouvement des données entre le client et la destination de stockage.
- **Cluster Veritas** : Partage un système de fichiers NFS avec les autres nœuds (serveurs) du réseau public
- **Cluster Oracle** : Représente une base de données Oracle mise en Cluster
- **Tape Library** : Représente un système de stockage qui contient plusieurs bandes et lecteurs de bandes magnétiques qui stockent des données à des fins de sauvegarde.
- **San Switches** : Est souvent utilisé par les entreprises pour les applications critiques qui nécessitent un débit élevé et une faible latence. Les SAN Switches utilisent la fibre optique pour transférer les données entre les serveurs et les périphériques de stockage. Ils permettent aux serveurs d'accéder aux ressources de stockage à distance.
- **Storage** : Est un équipement composé d'un ensemble de disques regroupés dont l'objectif principal est de fournir des espaces sécurisés de stockages vers des serveurs d'applications.
- **Cluster** : Groupe de serveurs indépendants qui sont gérés comme un système unique. Il est spécifiquement conçu pour tolérer les pannes des composants, et pour prendre en charge l'ajout ou la soustraction de composants d'une manière transparente pour les utilisateurs.

- **Catalogue** : Un groupe de fichiers contenant des informations vitales sur sauvegardes informations telles que la configuration, l'état, quels fichiers et dossiers ont été sauvegardés.

II.2.2. Contraintes et limitations de l'architecture

L'architecture existante chez l'entreprise « X » ne respecte pas les de sécurité RTO et RPO puisqu'à ce stade ces deux paramètres n'ont pas encore été définis, il est donc difficile de savoir combien de temps durera la reprise si jamais un sinistre venait à menacer l'activité de l'entreprise.

Les deux clusters sont très gourmands en matière de données : le cluster Oracle nécessite à lui seul une sauvegarde de 100 To. L'obstacle principal de sauvegarde est le fait que le flux de données soit entravé essentiellement au niveau des liens du réseau de sauvegarde (1Go).

Le périphérique de stockage (Tape Library) comporte deux bandes magnétiques, et donc ne peut effectuer que deux sauvegardes en parallèle. S'il y a besoin de faire une 3ème sauvegarde, il va falloir attendre qu'une bande se libère pendant un intervalle de temps indéterminé selon la durée de la sauvegarde.

Dans le cas de cette architecture, une opération de sauvegarde prend environs ***11 jours***, et donc ***16 à 17 jours*** de récupération de données, selon la loi de calcul du temps de récupération à partir du temps de sauvegarde définie par l'entreprise :

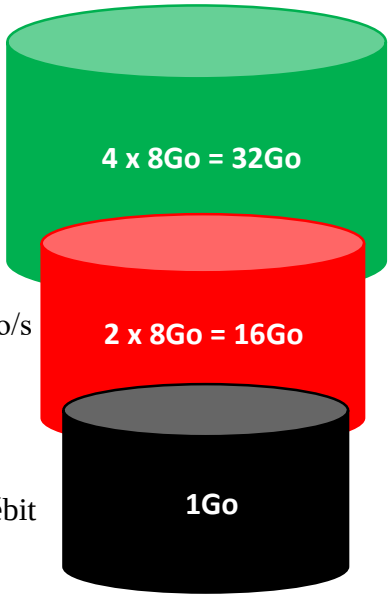
$$\mathbf{DR = DS + DS \div 2}$$

Tel que : **DR** = Durée de récupération

DS = Durée de sauvegarde

Le calcul du temps de sauvegarde est défini par la loi suivante :

Temps de sauvegarde = Taille des données ÷ Débit [15]



- Pour sauvegarder 100 To en Mégaoctets dans un réseau de sauvegarde 1Go, le débit théorique est de 128 Mo/s
  - 100 To ⟶ 100 000 Go
  - 100 000 Go ⟶ 100 000 000 Mo
  - 1 Mo ⟶ 1024 Ko ÷ 8 bits ⟶ 128 Ko/s
  - 1Go ⟶ 1000 Mo ⟶ 128 000 Ko/s
    ⟶ 128 Mo/s
- Un débit réaliste représente à peu près 80% du débit théorique
  - 128 Mo /s * 80% ⟶ 102,4 Mo/s
- Le temps estimé de sauvegarde sera de ***11,30 jours***
  - 100 000 000 Mo ÷ 102,4 Mo/s ⟶ 976 562,5 s
  - 976 562,5 s ⟶ 271,27 h
  - 271,27 h ⟶ ***11,30 jours***

- Ce délai est inadmissible pour la sauvegarde de données et la reprise en cas de désastre.

Les éléments cités en haut réduisent les performances de la sauvegarde / reprise et causent par conséquent un problème au sein du PRA. En effet si les données ne sont pas sauvegardées il y aura un impact direct sur la productivité de l'entreprise après sa reprise d'activité ce qui impliquera une chute de revenus, et donc des conséquences financières importantes pour l'entreprise.

II.3. Architecture optimisée

Comme première étape d'optimisation de l'architecture initiale de l'entreprise « X », il était impératif de définir les paramètres RTO et RPO.

Pour cela, nous nous sommes renseignées auprès des responsables des services critiques de l'entreprise sur la durée maximale d'interruption d'activité, et de l'intervalle de temps correspondant au volume maximal de perte données qu'ils jugeaient admissibles.

Sur la base de ces discussions, nous avons convenu de la valeur de 24h aux deux paramètres.

La deuxième étape était de proposer des changements techniques au niveau de l'architecture initiale de l'entreprise dans le but d'améliorer les débits et d'augmenter la vitesse et le nombre de sauvegardes (***Figure II.2***).

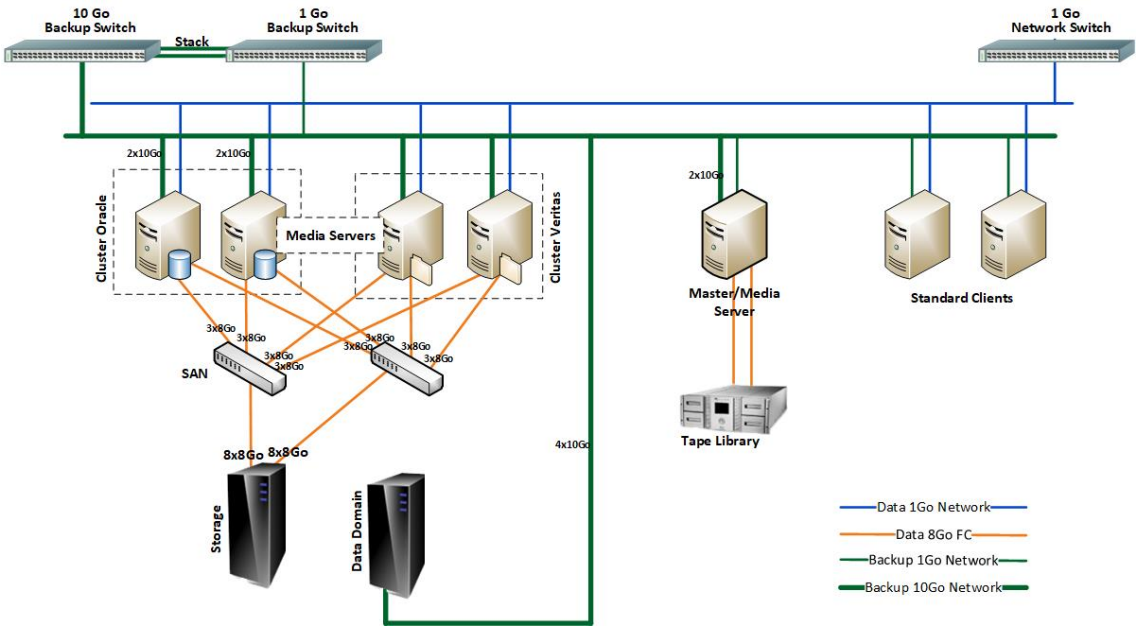


Figure II.2 : Solution d'architecture

Les modifications suivantes ont été suggérées :

- Un switch de sauvegarde de 10Go a été ajouté à l'architecture et empilé à l'ancien switch de sauvegarde (1Go).
- Les liaisons de 1Go entre les clusters et l'ancien switch de sauvegarde (1Go) ont été éliminées. De nouveaux liens (redondants) de 10Go ont été mis en place entre les clusters, le master serveur et le nouveau switch de sauvegarde (10Go).
- Ajout de liens 8Go FO entre : - Switches SAN – Storage (4 liens redondants)

  - Switches SAN – Serveurs (1 lien redondant)
- Agrégation des liens ajoutés (8x8Go=64Go, 3x8Go=24Go)
- Un nouveau média de sauvegarde remplaçant la Tape Library et permettant plusieurs sauvegardes en parallèle a été mis en place : le Data Domain Storage.
- Le Data Domain Storage est un système de stockage avec déduplication.

- Les serveurs en cluster ont été transformés en Média Serveurs afin de réaliser une sauvegarde directe de données dans le Data Domain sans passer par le Master Serveur (le mécanisme d'installation des Master / Médias serveurs est détaillé en Annexe).
- Les anciens liens de sauvegardes (1Go) ont été gardés dans le but d'effectuer les sauvegardes des clients standards (serveurs moins gourmands).
- Les sauvegardes des clients standards transitent par le Master Serveur (qui garde toujours sa faculté de média Serveur) avant d'être stockées dans le Data Domain.
- La Tape Library sert dorénavant à archiver les catalogues du Master Serveur.

Pour réduire encore plus le temps de sauvegarde et par conséquent celui de la reprise d'activité, nous nous sommes informées auprès des responsables de services critiques, sur le volume de données indispensable à récupérer pour que l'entreprise puisse reprendre son activité en mode dégradé dans le but de ne pas dépasser le RTO défini et pour limiter le temps d'inaction de l'entreprise. La récupération du reste de données se fait graduellement, durant le processus de reprise d'activité.

Une valeur de ***30To*** a été attribuée à ce volume de données ce qui correspond à ***3 mois*** de travail.

La sauvegarde prendra donc une durée de ***2 heures*** et la récupération de données durera ***3 heures***.

- Les 30 To de données de sauvegarde sont exprimés en Mégaoctets, le nouveau réseau de sauvegarde peut transférer jusqu'à 40 Go de données, donc le débit théorique est de 5120 Mo/s.
  - 30 To ⟶ 30 000 Go
  - 30 000 Go ⟶ 30 000 000 Mo
  - 1 Mo ⟶ 1024 Ko ÷ 8 bits ⟶ 128 Ko/s
  - 40Go ⟶ 40 000 Mo ⟶ 5120 000 Ko/s
    ⟶ 5120 Mo/s
- La valeur du débit réaliste est 4096 Mo/s
  - 5120 Mo /s * 80% ⟶ 4096 Mo/s

- 30 000 000 Mo ÷ 4096 Mo/s ⟶ 7324,21875 s

o Le délai de sauvegarde de 30 To de données sera donc de ***2,03h***

- 7324,21875 s ⟶ ***2,03 h***

La sauvegarde servira essentiellement à dupliquer et protéger les données sur un support indépendant afin de pouvoir les récupérer en cas de sinistre. Pour ce faire, deux types de sauvegardes vont être effectués à fréquences différentes.

- **Sauvegarde complète :** Est programmée une fois par semaine, elle fait une copie de toutes les données de l'entreprise et requiert beaucoup de temps et d'espace de stockage.
- **Sauvegarde incrémentale :** Est effectuée à une fréquence quotidienne, elle réalise une sauvegarde complète de données le premier jour puis ne stocke que les fichiers mis à jour (ajoutés, modifiés, supprimés) par rapport à la sauvegarde précédente.

Ces deux sauvegardes permettront de diminuer le volume de perte de données qui correspondra toujours à un intervalle de temps inférieur ou égal à ***24h***, cela signifie que dans le pire des cas ***24h*** de données seront perdues, donc le paramètre RPO est respecté.

Nous réussissons ainsi à améliorer le temps de sauvegarde et par conséquent celui de la récupération de données, en allant d'un délai de sauvegarde de 11 jours jusqu'à un délai de 2h qui respecte le paramètre RPO, et d'une durée de récupération de 16 jours, jusqu'à une durée de 3h qui respecte le paramètre RTO défini.

II.4. Conclusion

Cette solution a été entièrement validée et approuvée par le responsable de la stratégie de sauvegarde de l'entreprise et constitue une confirmation de la solution adoptée qui est actuellement fonctionnelle au sein de l'entreprise « X ».

La définition d'objectifs de reprise RTO et RPO et de stratégies de sauvegarde joue un rôle crucial dans l'élaboration d'un PRA, car ces éléments ont un impact direct sur le processus de reprise d'activité après un sinistre.

CHAPITRE III Reprise d'activité après sinistre en utilisant Relax and Recover

III.1. Introduction

III.2. Outils et simulation

III.2.1.Définition

III.2.2.Configurer la sauvegarde ReaR avec la méthode NFS

III.3. Conclusion

CHAPITRE III : Reprise d'activité après sinistre en utilisant Relax and Recover

III.1. Introduction

Ce chapitre porte sur la simulation de reprise d'activité après sinistre à petite échelle en utilisant l'outil ReaR dans un environnement virtuel à l'aide du logiciel VMware Workstation Pro sous une machine virtuelle CentOS 7.

III.2. Outils et simulation

III.2.1. Définition

Relax-and-Recover (ReaR) est une solution open source de reprise après sinistre entièrement écrit en bash conçue pour les systèmes Linux. L'outil produit une image amorçable qui peut recréer la disposition de stockage d'origine du système. Une fois cela fait, il lance une restauration à partir de la sauvegarde.

III.2.2. Configurer la sauvegarde ReaR avec la méthode NFS

Avant de configurer ReaR, un plan de sauvegarde/restauration doit être établi :

- Configurer un Serveur NFS pour stocker les fichiers de sauvegarde.
- Choisir une méthode de récupération pour créer un système de secours / récupération.

➢ **Configuration NFS**

- **Serveur NFS (*N*etwork *F*ile *S*ystem)**

  En pratique, l'utilisateur, à partir de son ordinateur, va pouvoir accéder à des fichiers stockés sur un serveur distant, à l'aide du protocole NFS qui fonctionne selon le mode client/serveur.

- **Services importants**

  Rpcbind : le rpcbind convertit les numéros de programme RPC en adresses universelles.

  Nfs-server : permet aux clients d'accéder aux partages NFS

- **Fichiers de configuration**

  /etc/exports : est un fichier de configuration qui contrôle quels systèmes de fichiers sont exportés vers des hôtes distants et spécifie les options.

  /etc/fstab : Utilisé pour contrôler le montage des systèmes de fichiers y compris les répertoires NFS lorsque le système redémarre.

Le scénario de la simulation est le suivant : nous voulons garantir la reprise d'activité de la ***Machine 1*** qui est exposée à un risque susceptible d'endommager son système et de causer la perte de ses données. Comme mesure préventive, nous allons lancer un processus de sauvegarde à l'aide de l'outil **ReaR** qui va créer un support de récupération (**image ISO**), au niveau de la ***Machine 2*** en utilisant le protocole **NFS**, contenant des fichiers de secours et de sauvegarde du système de la ***Machine 1***.

Une fois le système de récupération est créé, nous allons volontairement endommager la ***Machine 1***, et tenter de récupérer son système à partir de l'image amorçable (ISO) créée.

Le processus d'installation et de configuration du service NFS est illustré dans les figures [***III.1 - III.6***].

Machine 1 :

1. Installation NFS:

```
# yum install nfs-utils
```

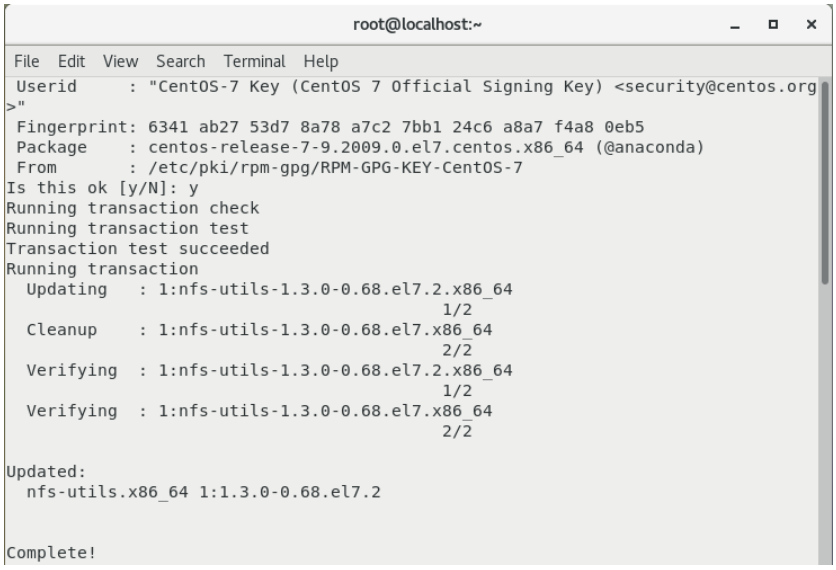


Figure III.1 : Installation NFS sur la Machine 1

2. Une fois les packages installés, activer and démarrer les services NFS :

```
# systemctl enable rpcbind
# systemctl enable nfs-server
# systemctl start rpcbind
# systemctl start nfs-server
```

3. Créer le répertoire /storage afin de stocker les fichiers de sauvegarde ultérieurement.

```
# mkdir /storage
```

4. Accorder les permissions de “lecture, écriture, exécution” au répertoire précédant.

```
# chmod 775 /storage
```

5. Vérifier l’adresse IP de la machine NFS Server :

```
# ifconfig
```

6. Ouvrir le fichier ***/etc/exports*** avec l’éditeur vi :

```
# vi /etc/exports
```

7. Ecrire dans le fichier ***/etc/exports*** :

```
/storage
*(fsid=0,rw,sync,no_root_squash,no_subtree_check,crossmnt)
```

8. Autoriser le trafic à accéder aux services nfs rpc-bind :

```
# firewall-cmd --permanent --add-service mountd
# firewall-cmd --permanent --add-service rpc-bind
# firewall-cmd --permanent --add-service nfs
# firewall-cmd --reload
```

9. Réexporter tous les répertoires après modification de ***/etc/exports*** :

```
# exportfs -r
```

10. Monter le fichier partagé :

```
# showmount –e localhost
```

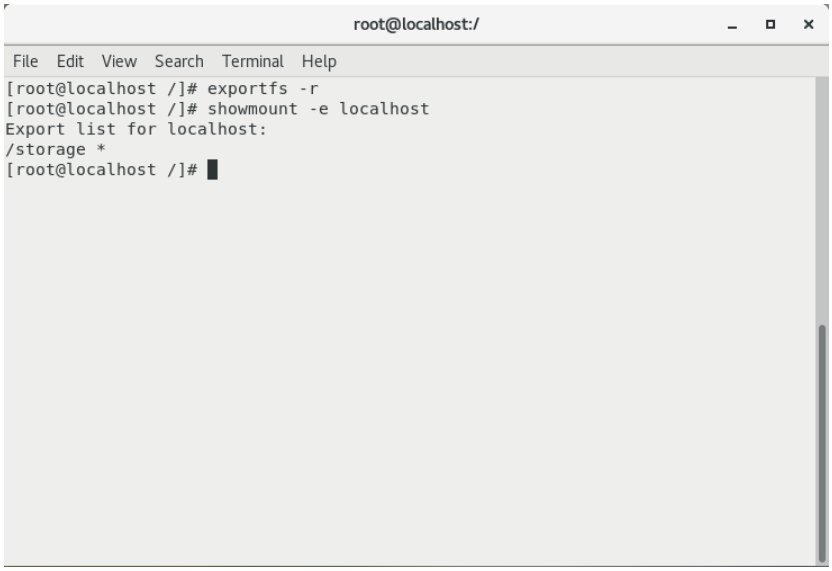


Figure III.2 : Liste de fichiers partagés NFS

Machine 2:

11. Installation NFS :

```
# yum install nfs-utils
```

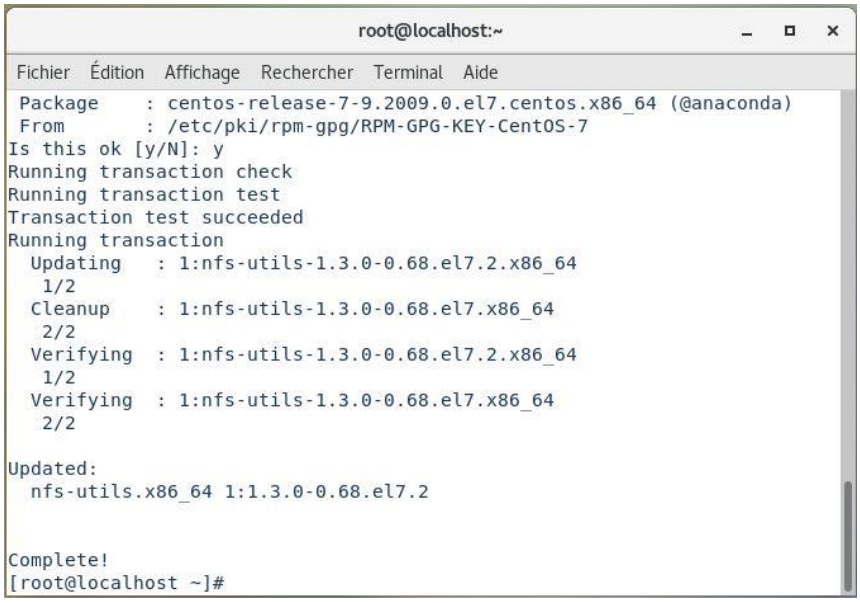


Figure III.3 : Installation NFS sur la Machine 2

12. Une fois les packages installés, activer and démarrer les services NFS :

```
# systemctl enable rpcbind
# systemctl enable nfs-server
# systemctl start rpcbind
# systemctl start nfs-server
```

13. Avant de monter les fichiers partagés, vérifier d'abord quels sont les fichiers partagés du Serveur NFS :

```
# showmount -e 192.168.38.128
```

14. Créer un point (répertoire) de montage (/storageC) dans lequel va se retrouver le répertoire partagé (/storage) créé dans le Serveur NFS :

```
# mkdir /storageC
# mount -t nfs 192.168.38.128:/storage /storageC
```

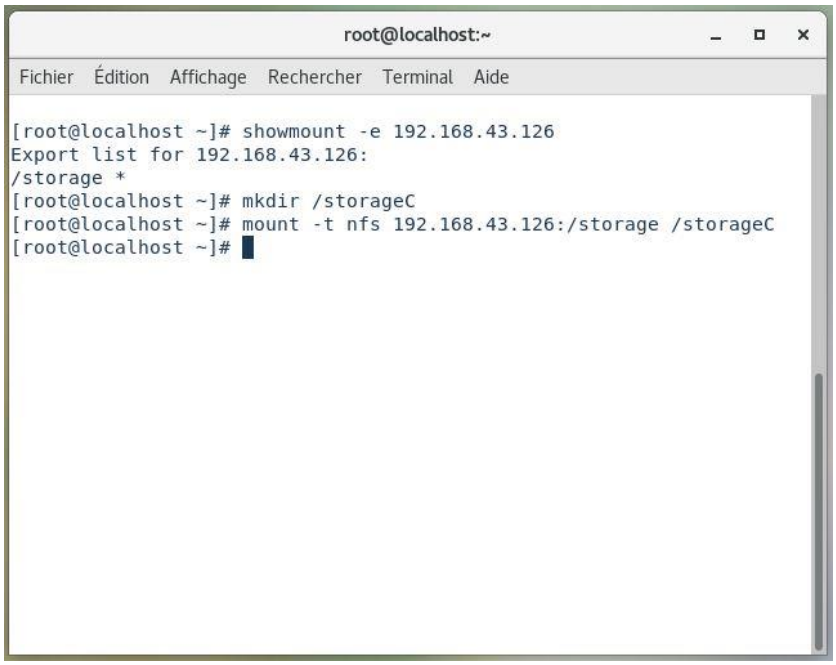


Figure III.4 : Montage de système de fichiers

15. Afin de contrôler le partage de fichier au redémarrage :

- Ouvrir le fichier ***/etc/fstab*** :

```
# vi /etc/fstab
```

- Ecrire dans le fichier ***/etc/fstab*** :

```
192.168.38.128:/storage /storageC nfs
nosuid,rw,sync,hard,intr 0 0
```

16. Tester la création de fichier dans les deux machines Client et Serveur :

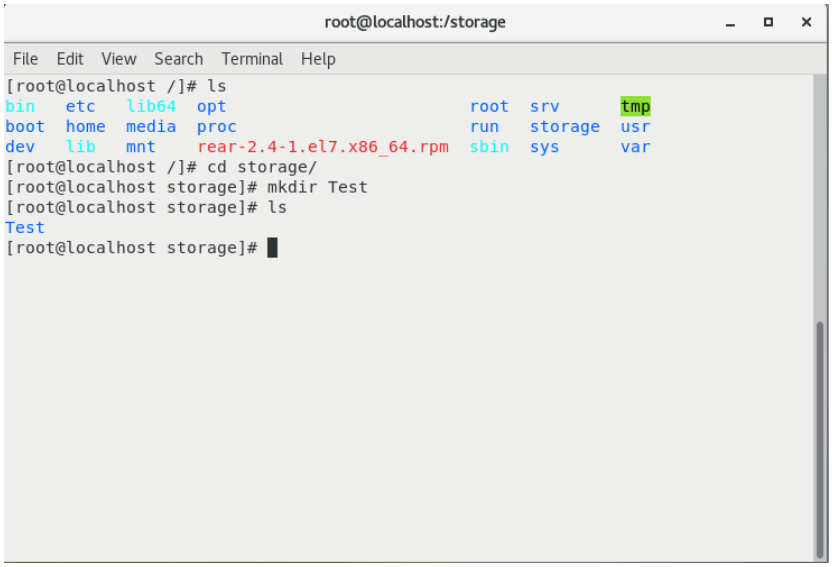


Figure III.5 : Test du système de fichiers NFS sur la Machine 1

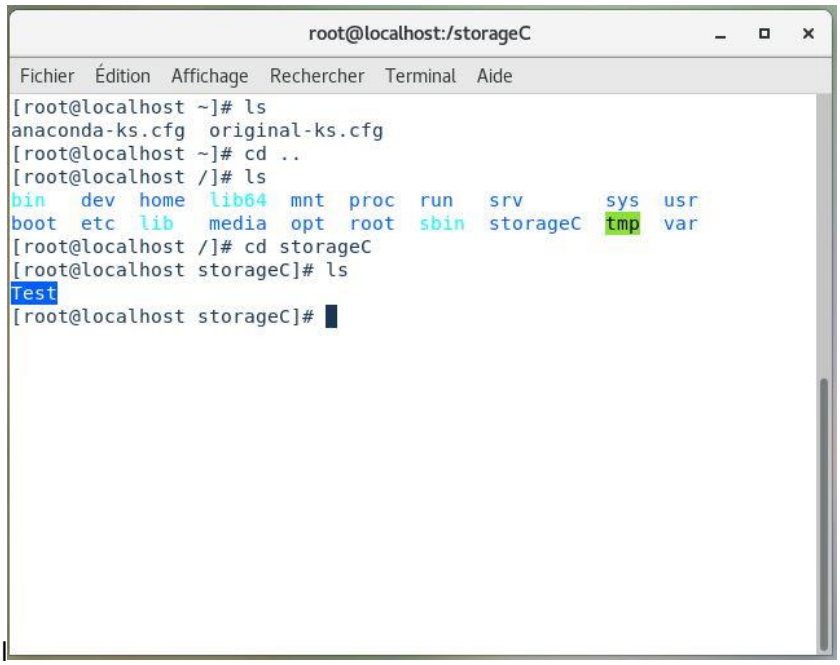


Figure III.6 : Test du système de fichiers NFS sur la Machine 2

- **Installation et Configuration ReaR**

Le processus d'installation et de configuration ReaR est illustré dans les figures [***III.7 - III.20]***.

Machine 1:

1. Installer ReaR : importer le Package d'installation ReaR et lancer l'installation :

```
#yum install /rear-2.4-1.el7.x86_64.rpm
```

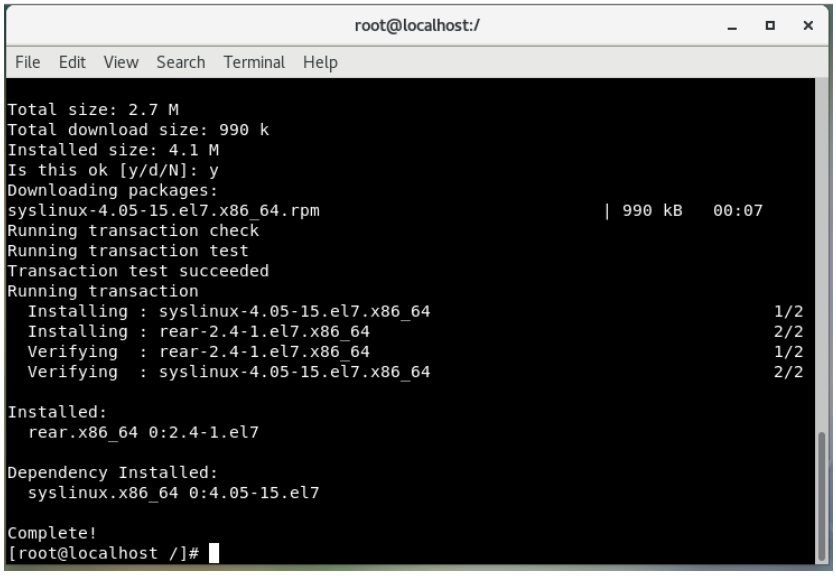


Figure III.7 : Installation ReaR

2. Afin de configurer ReaR, il faut modifier et ajouter des options spécifiques (qui vont être détaillées ci-dessous) au fichier ***/etc/rear/local.conf***

```
vi /etc/rear/local.conf
```

```
OUTPUT=ISO
OUTPUT_URL=nfs:///storage/
BACKUP=NETFS
BACKUP_URL=iso:///storage/
```

Les options de configuration de la sauvegarde ReaR sont définies au niveau du fichier ***/etc/rear/local.conf*** selon les besoins de l'utilisateur, pour notre simulation nous avons choisi les options suivantes :

OUTPUT=ISO : Pour créer un système de secours dans une image ISO amorçable sur le disque

OUTPUT_URL=nfs:///storage/ : Fournit l'emplacement cible d'image ISO, en utilisant le protocole NFS

BACKUP=NETFS : Décrit la méthode/stratégie du BACKUP (aussi appelée méthode de sauvegarde interne, l'option NETFS permet de créer un système de secours ET une sauvegarde complète)

BACKUP_URL=iso:///storage/ : Définit l'emplacement où stocker la sauvegarde (dans notre exemple : le système de secours et la sauvegarde se trouvent dans l'image ISO) → il s'agit de la méthode la plus simple de sauvegarde complète du système, car le système de secours n'a pas besoin que l'utilisateur récupère la sauvegarde pendant la restauration.

3. Lancer la sauvegarde qui permet de créer un système de secours et de sauvegarde via la commande :

```
#rear -v mkbackup
```

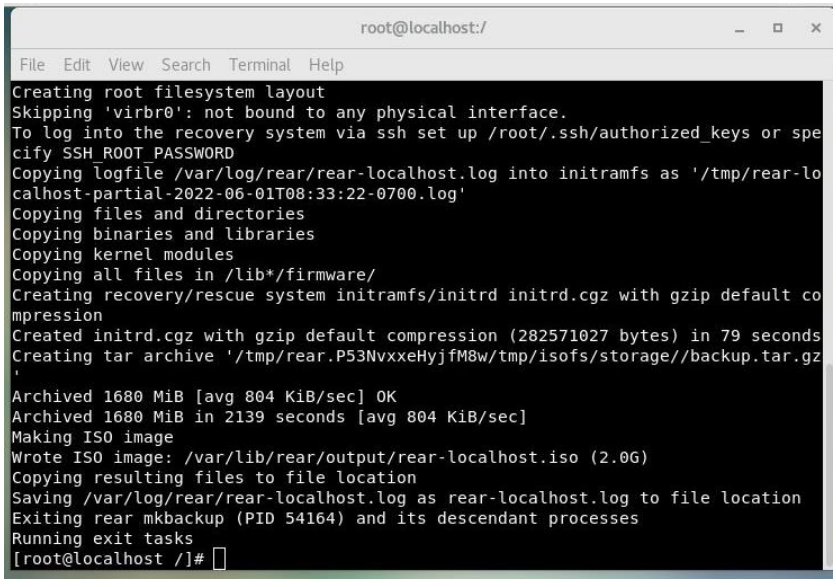


Figure III.8 : Création de système de secours et de sauvegarde

4. Afficher les fichiers générés après sauvegarde dans le répertoire /storage

```
#ll -h /storage/localhost
```

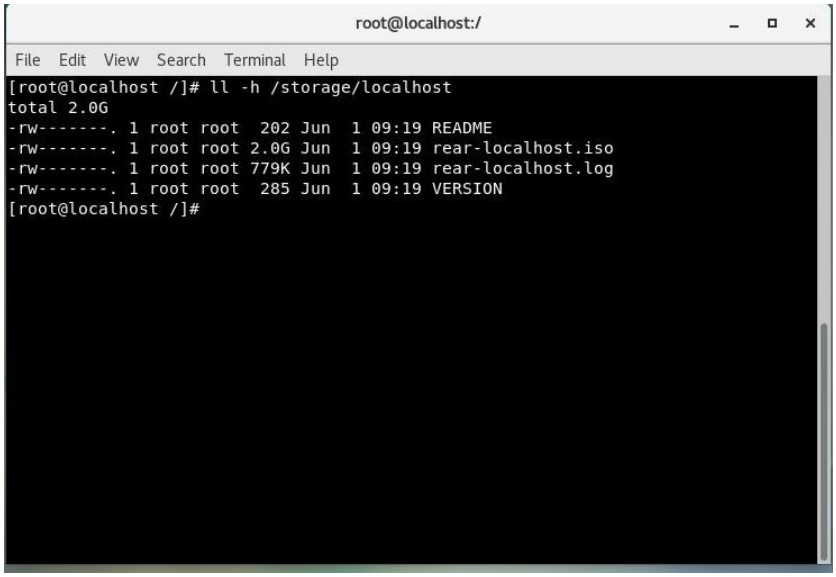


Figure III.9 : Contenu du fichier de récupération ReaR

Machine 2 :

5. Afficher les fichiers générés après sauvegarde dans le répertoire /storageC grâce au protocole NFS

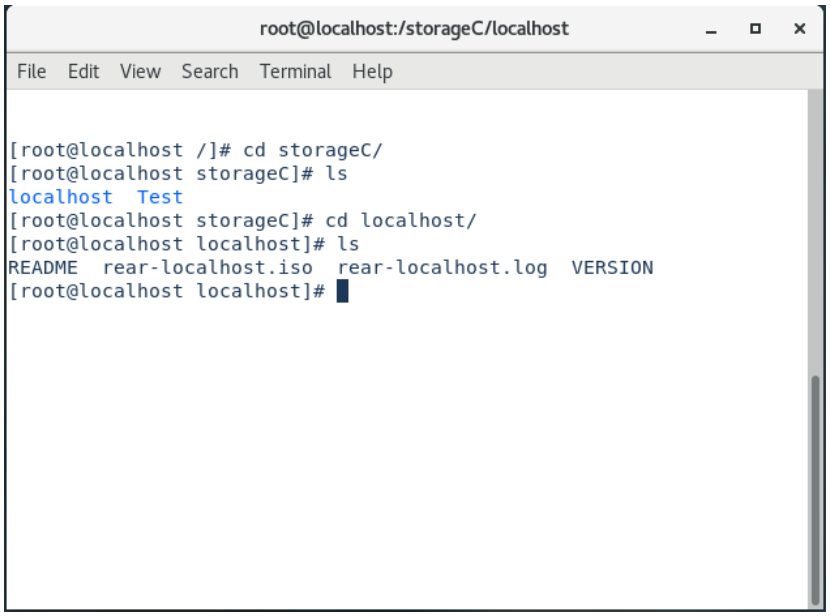


Figure III.10 : Contenu du répertoire monté par NFS

Machine 1 :

6. Endommager le système (effacer le root)

```
#rm -rf /*
```

7. Redémarrer la MV

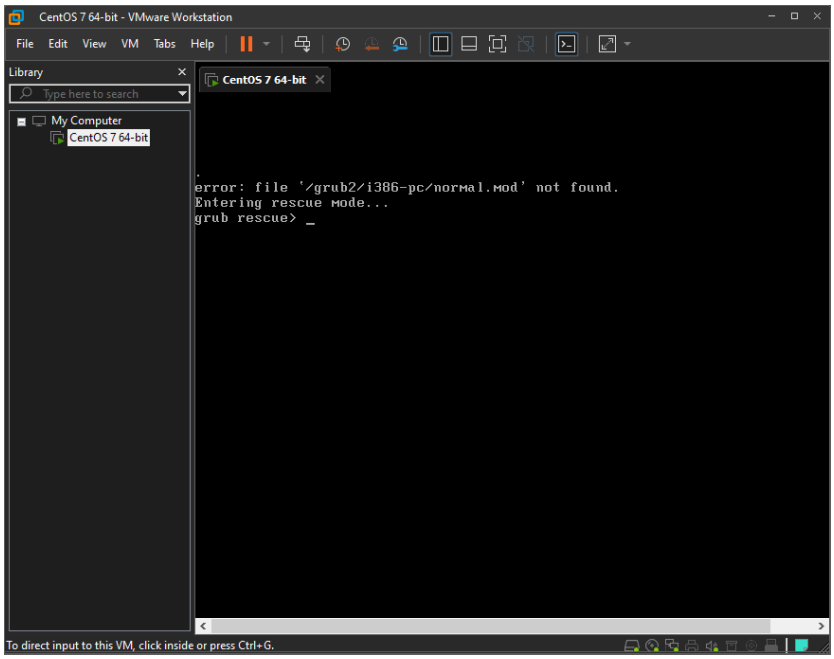


Figure III.11 : Système endommagé

➢ **Récupération du système**

Machine 2:

1. Copier le système de secours et de sauvegarde dans une Clé USB

```
#cp -R /storageC/localhost /run/media/imane/B4DD-C581
```

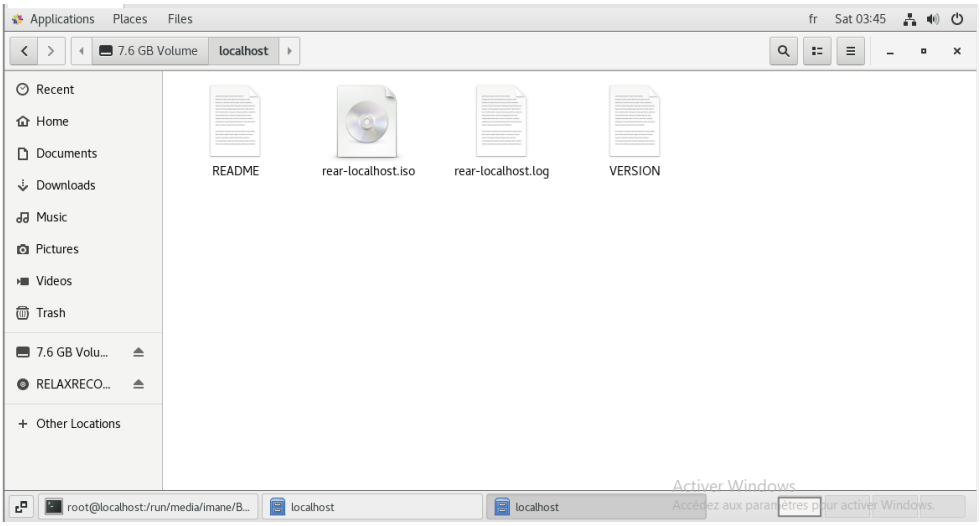


Figure III.12 : Copie du système dans un support de stockage

Machine 1 :

2. Afin de pouvoir amorcer le système à partir de l'image ISO créée, il faudra l'importer dans le système de base (lecteur CD/DVD) de la VM

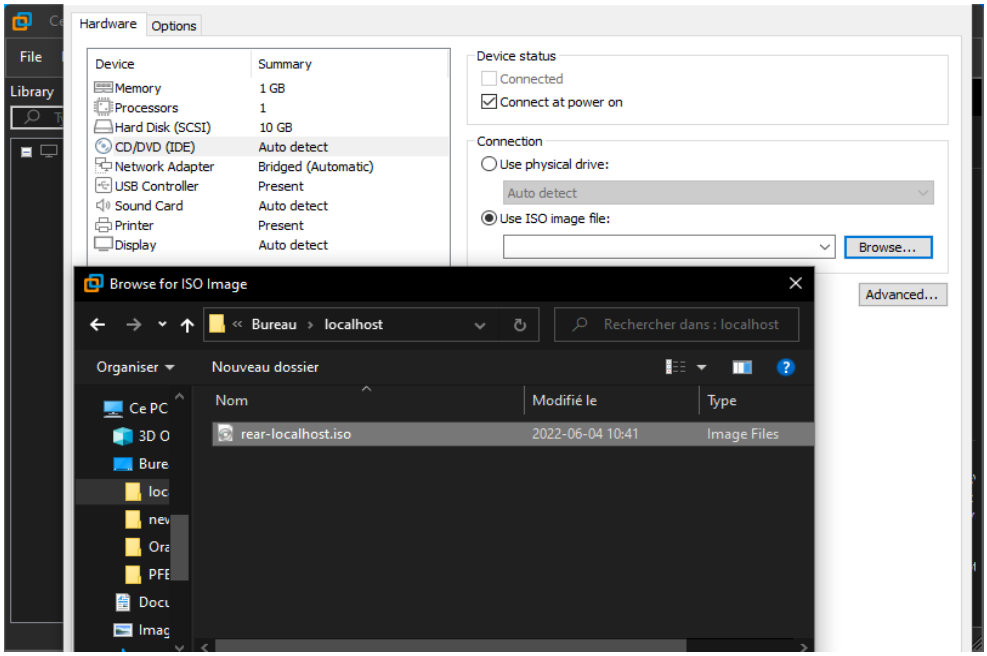


Figure III.13 : Importation de l'image ISO

3. Démarrer la MV à partir du BIOS (en sélectionnant l'option « Power On to Firmware »), puis suivre les étapes indiquées pour pouvoir redémarrer la MV à partir du CD-ROM.

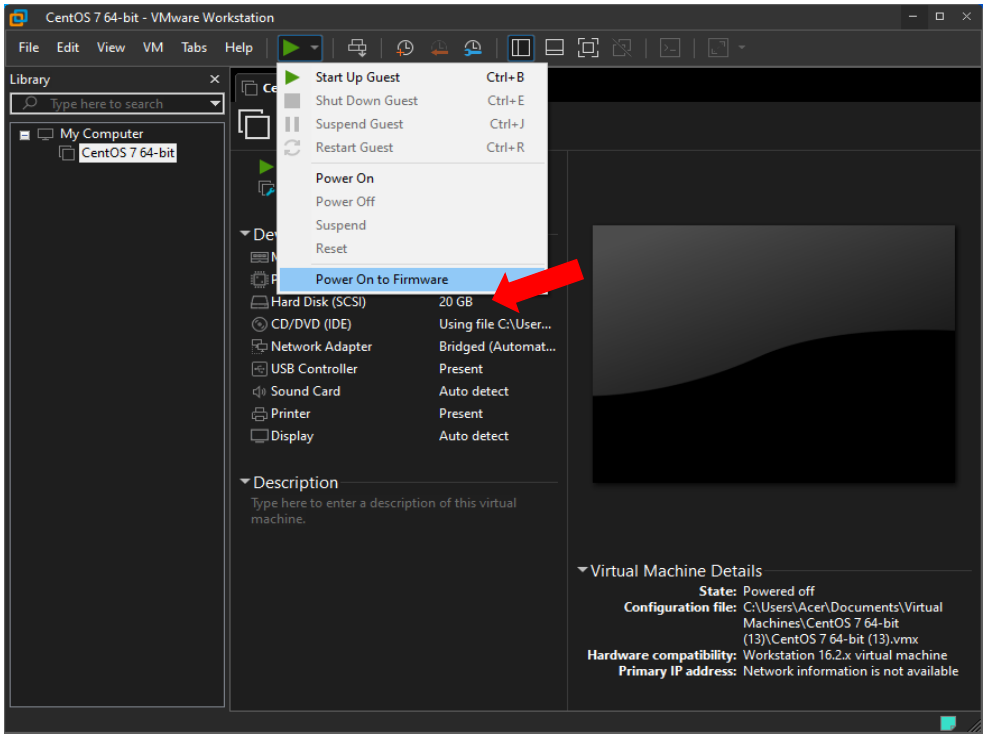


Figure III.14 : Démarrage en mode BIOS

4. Choisir CD-ROM drive comme option de démarrage, puis sauvegarder la configuration

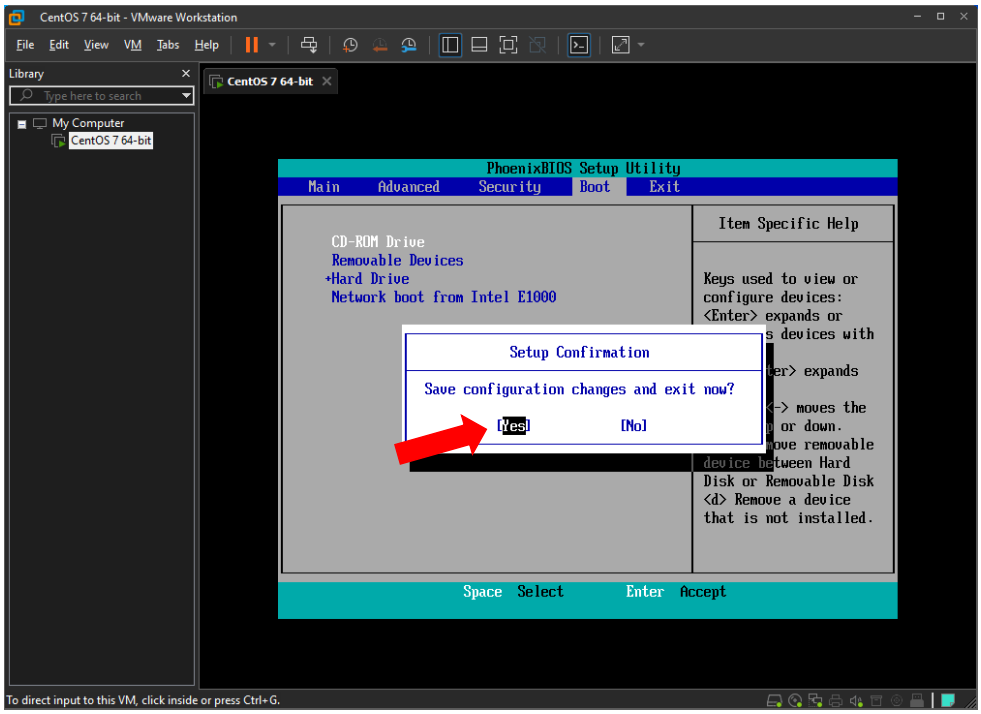


Figure III.15 : Sauvegarde de la configuration

4. La MV redémarre (à partir du système de secours présent dans l'image ISO) et affiche le menu ReaR. L'option *Recover localhost* est sélectionnée.

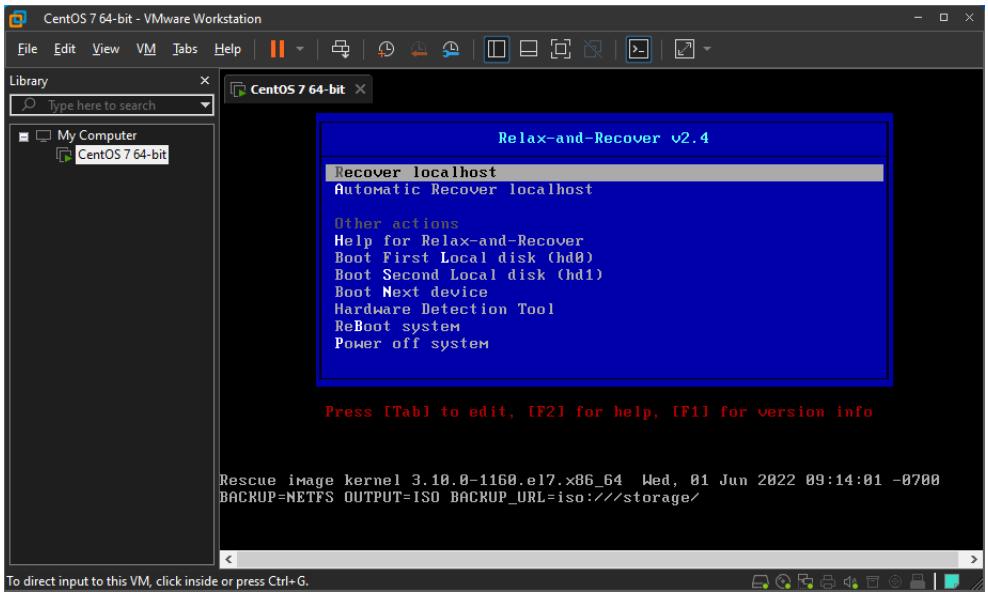


Figure III.16 : Démarrage en mode secours ReaR

5. Se connecter en mode root
6. Lancer la reprise (recovery) du système à travers la commande

```
#rear recover
```

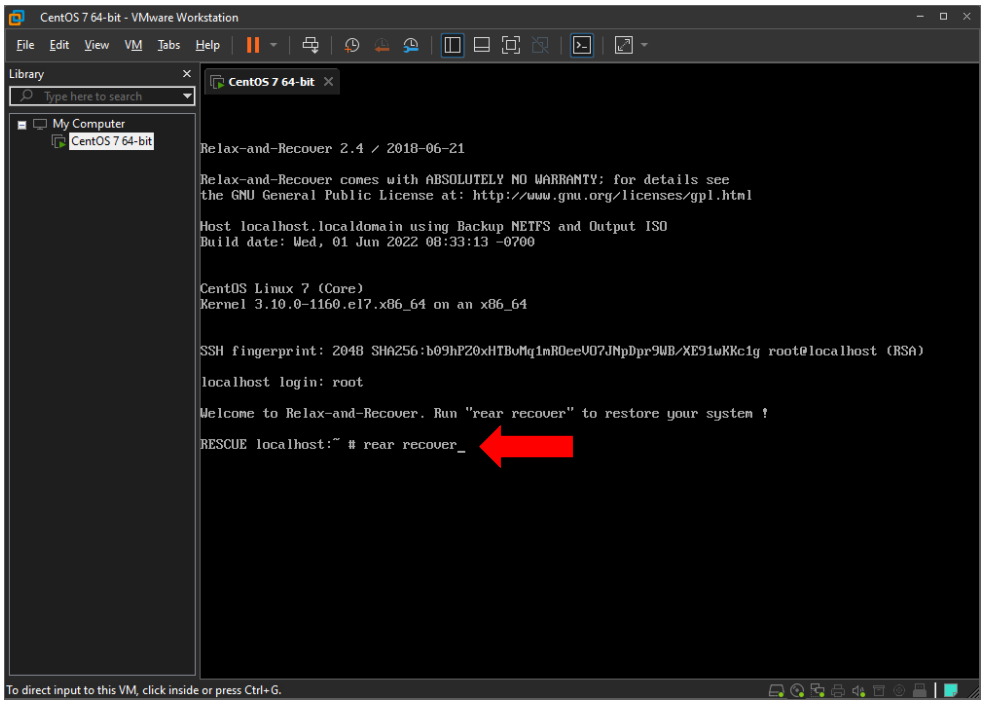


Figure III.17 : Lancer la reprise du système

7. Redémarrer la MV en utilisant la commande ***reboot***

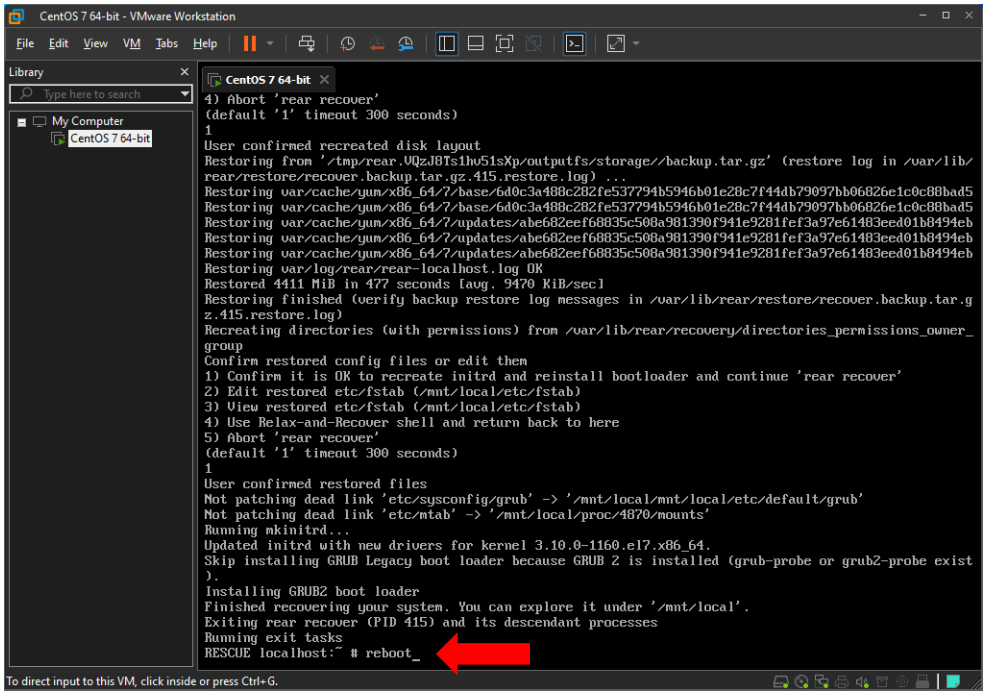


Figure III.18 : Redémarrage de la MV

8. Démarrer la MV à partir du disque (hd0)

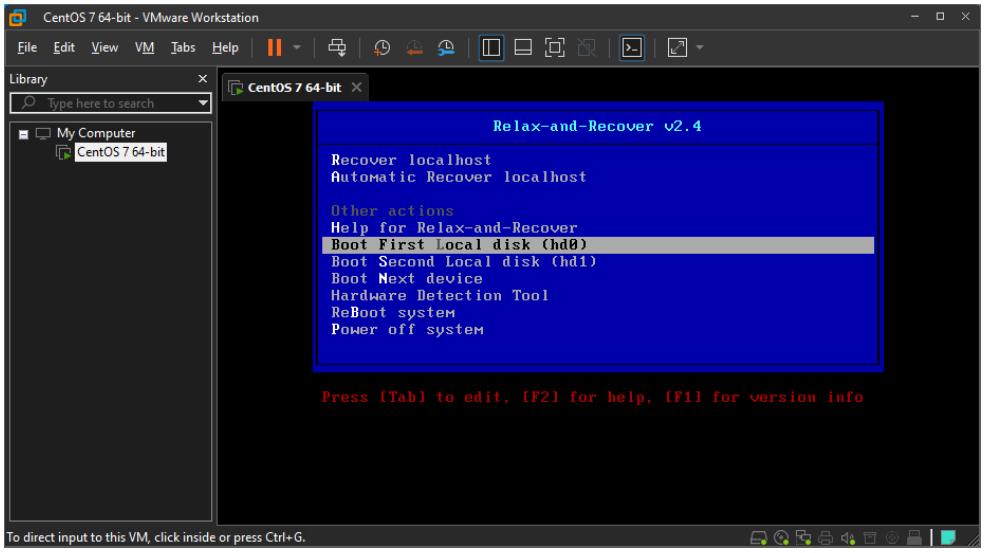


Figure III.19 : Redémarrage du Machine 1

9. La MV reprend son activité en redémarrant à partir du système de récupération ReaR.

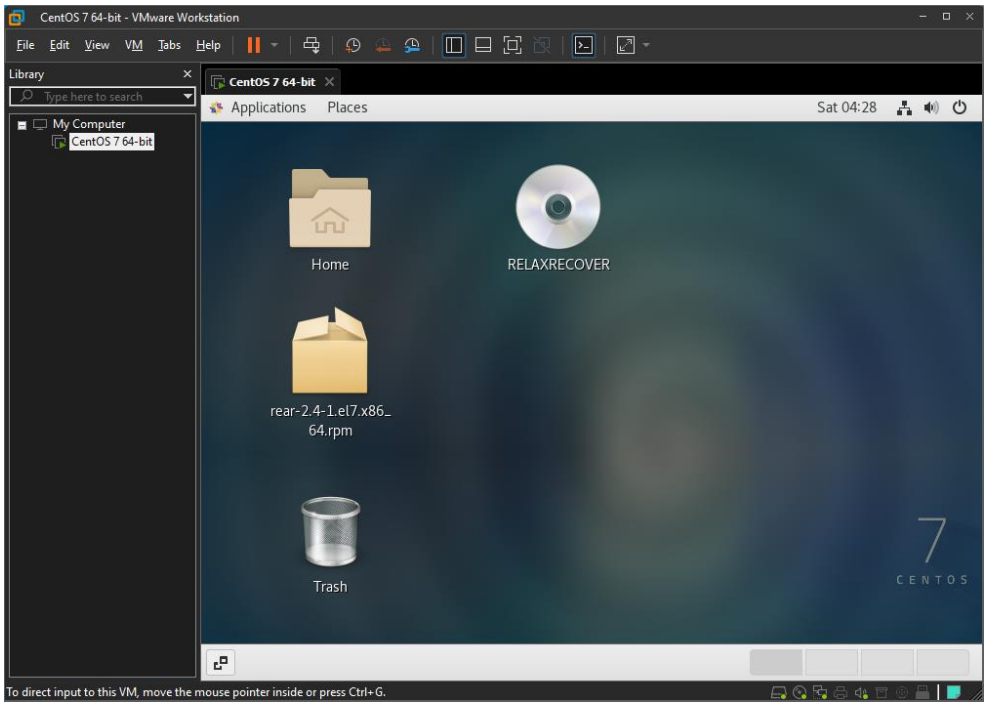


Figure III.20 : Système récupéré

III.3. Conclusion

L'outil ReaR peut fonctionner sous n'importe quel environnement Linux grâce à ses étapes et paramètres de configuration (de 1 jusqu'à 9) permettant la création d'un système de secours à partir duquel une machine peut récupérer son système et par conséquent reprendre son activité.

Conclusion générale

Nous avons essayé, tout au long de ce travail, de présenter les aspects de la mise en œuvre d'un plan de reprise d'activité, en commençant par décrire l'étude d'analyse de risque et les différentes stratégies adoptées pour l'élaboration d'un PRA , puis nous avons proposé une solution de sauvegarde adaptée à un cas de figure, et finalement nous avons réalisé une simulation d'interruption puis de reprise d'activité.

Nous avons tenté d'être aussi exhaustives que possible, mais il va sans dire que le PRA a un périmètre très large et contient une infinité de scénarios et de possibilités dans la solution à mettre en place. Ainsi toute entreprise voulant élaborer un PRA doit adapter les solutions et méthodes appliquées à son environnement et à la configuration de ses systèmes d'information.

Bien que notre travail atteigne les objectifs que nous nous sommes fixés tout au long du délai imparti à la réalisation de ce mémoire, Nos futures perspectives seraient de réaliser un PRA avec toutes ses étapes et composantes adapté à une entreprise, et pouvoir développer et améliorer ses stratégies selon les besoins de cette entreprise.

Bibliographie

[1] Adenium-brg, «MISE EN OEUVRE D'UN PLAN DE REPRISE D'ACTIVITÉ (PRA),» [En ligne]. Available: https://www.adenium.fr/blog/mise-en-oeuvre-d-un-plan-de-reprise-d-activite-pra/.

[2] Value IT, «Plan de reprise d'activité : comment le mettre en place,» [En ligne]. Available: https://www.value-info.fr/plan-de-reprise-d-activite-comment-le-mettre-en-place/.

[3] I. Bagan, Patrick Bauthéac, Danilo Bilotta, Agostino Goretti et Régis Thépot, «Programme 2018-2019 de revue par les pairs dans le cadre de la coopération de l'UE en matière de protection civile et de gestion des risques de catastrophe.,» 2018-2019.

[4] Bureau Régional de l'UNISDR pour les Pays Arabes, «Pour une Algérie Résiliente Réaliser la Réduction des Risques de Catastrophe dans les Pays Arabes: Etude Nationale sur les Bonnes Pratiques,» 2013.

[5] M. Ruel et Michel Pérusse, «Les 4 T de la gestion des risques,» [En ligne]. Available: https://travailetsante.net/articles/les-4-t-de-la-gestion-des-risques/.

[6] M. Amellah, «Gestion des risques projet : 7 étapes et 4 stratégies à mettre en place,» [En ligne]. Available: https://blog-gestion-de-projet.com/gestion-des-risques-projet/.

[7] M. SENE, «La gestion et le traitement des risques,» [En ligne]. Available: https://www.linkedin.com/pulse/la-gestion-et-le-traitement-des-risques-moustapha-sene/?originalSubdomain=fr.

[8] Nuabee, «Comprendre les termes RPO et RTO dans un projet de PRA,» [En ligne]. Available: https://nuabee.fr/blog/comprendre-les-termes-rpo-et-rto?fbclid=IwAR2RypfFIJoLAnInqfd-zR0XR5ZH8Yn4hANORqDrS3s4Cb8LR9IHboq4m-Y.

[9] P. Crocetti, «site de reprise après sinistre (site DR),» [En ligne]. Available: https://www.techtarget.com/searchdisasterrecovery/definition/disaster-recovery-site-DR-site#:~:text=A%20disaster%20recovery%20(DR)%20site,primary%20data%20center%20becomes%20unavailable..

[10] Digital Guide IONOS, «Cloud Disaster Recovery : être bien préparé en cas de sinistre,» [En ligne]. Available: https://www.ionos.fr/digitalguide/serveur/securite/cloud-disaster-recovery/.

[11] J. Moore, «Guide DRaaS : avantages, défis, fournisseurs et tendances du marché,» [En ligne]. Available: https://www.techtarget.com/searchdisasterrecovery/DRaaS-guide-Benefits-challenges-providers-and-market-trends.

[12] E. Lecha et Matías Balzamo, «LEAF SPINE VS TRADITIONAL ARCHITECTURE,» [En ligne]. Available: https://blogs.salleurl.edu/en/leaf-spine-vs-traditional-architecture#:~:text=Leaf%20spine%20takes%20advantage%20of,to%20expand%20the%20available%20bandwidth.

[13] Huawei Enterprise Support Community, «Spine-Leaf vs Three-Tier Network Architecture,» [En ligne]. Available: https://forum.huawei.com/enterprise/en/spine-leaf-vs-three-tier-network-architecture/thread/782313-100723.

[14] J. Slaughter et Shree Rathinasamy, «Leaf-Spine Deployment and Best Practices Guide,» Dell EMC Networking Solutions Engineering, 2017.

[15] Anatoly Zolotkov, «Calcul de transfert de données,» [En ligne]. Available: https://www.translatorscafe.com/unit-converter/fr-FR/calculator/data-transfer-time/.

[16] Veritas, «Configuration NetBackup Master Server,» [En ligne]. Available: https://www.veritas.com/support/en_US/doc/24437881-126559615-0/v41275697-126559615.

[17] Veritas, «Installation du logiciel NetBackup Master Server sous UNIX,» [En ligne]. Available: https://www.veritas.com/support/en_US/doc/27801100-127350444-0/v13834345-127350444.

[18] Veritas, «Installation du logiciel NetBackup Media Server sous UNIX,» [En ligne]. Available: https://www.veritas.com/support/en_US/doc/27801100-127350444-0/id-SF890399007-127350444.

[19] Symantec, «Définition Enterprise Media Manager,» [En ligne]. Available: http://systemmanager.ru/nbadmin.en/ch31s02s02s01.htm.

[20] Qualitisio, «Les Risques : définition, types, évaluation et gestion,» [En ligne]. Available: https://www.qualitiso.com/risques-definition-types-evaluation-gestion/.

[21] CCHST - Centre Canadien d'Hygiène et de Sécurité au Travail, «Évaluation des risques,» [En ligne]. Available: https://www.cchst.ca/oshanswers/hsprograms/risk_assessment.html.

[22] T. Hanna, «Top 4 Types of Disaster Recovery Plans,» [En ligne]. Available: https://solutionsreview.com/backup-disaster-recovery/top-three-types-of-disaster-recovery-plans/.

[23] T. SMITH, «Disaster Recovery Site,» [En ligne]. Available: https://www.investopedia.com/terms/d/disaster-recovery-site.asp.

[24] B. BORSALLI, «8 étapes pour la gestion des risques SST,» [En ligne]. Available: https://blog.softexpert.com/fr/gestion-des-risques-sst/.

[25] S. J. Bigelow et Dave Raffo, «reprise après sinistre cloud (DR cloud),» [En ligne]. Available: https://www.techtarget.com/searchdisasterrecovery/definition/cloud-disaster-recovery-cloud-DR.

[26] Relax and Recover, «Relax-and-Recover,» [En ligne]. Available: https://relax-and-recover.org/.

[27] A. Putt, «Relax-and-Recover on RHEL,» [En ligne]. Available: http://www.softpanorama.org/Admin/Backup/Relax_and_restore/index.shtml.

[28] SUSE, «24 Disaster Recovery with Relax-and-Recover (Rear),» [En ligne]. Available: https://documentation.suse.com/sle-ha/12-SP4/html/SLE-HA-all/cha-ha-rear.html.

Liste d’abréviations

PRA	**P**lan de **R**eprise d’**A**ctivité
DRP	**D**isaster **R**ecovery **P**lan
RTO	**R**ecovery **T**ime **O**bjective
RPO	**R**ecovery **P**oint **O**bjective
Cloud DR	**Cloud D**isaster **R**ecovery
DMIA	**D**urée **M**aximale d’**I**nterruption **A**dmissible
PDMA	**P**erte de **D**onnées **M**aximale **A**dmissible
SAN	**S**torage **A**rea **N**etwork
NBU	**NetBackup**
DRaaS	**D**isaster **R**ecovery **as a S**ervice
ReaR	**Relax and Recover**
NFS	**N**etwork **F**ile **S**ystem
MV	**M**achine **V**irtuelle
IDS	**I**ntrusion **D**etection **S**ystems
IPS	**I**ntrusion **P**revention **S**ystems
STP	**S**panning **T**ree **P**rotocol
VTL	**V**irtual **L**ink **T**runking
ECMP	**E**qual **C**ost **M**ulti **P**ath Routing
FO	**F**ibre **O**ptique

Liste des figures

Figure I.1 : Cycle de vie 13
Figure I.2 : Processus d'étude de risques 14
Figure I.3 : Liste de risques identifiés en Algérie 15
Figure I.4 : Position du RTO/RPO pendant un sinistre 20
Figure I.5 : Topologie Leaf Spine 25
Figure I.6 : Topologie Traditionnelle 26
Figure I.7 : Layer 3 Leaf-Spine 2-Tiers Topologie : Centre de Données 27
Figure I.8 : Layer 2 Leaf-Spine 2-Tiers Topologie : Centre de reprise 28
Figure I.9 : Architecture proposée du centre de données 30
Figure I.10 : Architecture proposée du centre de reprise 30
Figure II.1 : Architecture de l'entreprise X 33
Figure II.2 : Solution d'architecture 37
Figure III.1 : Installation NFS sur la Machine 1 42
Figure III.2 : Liste de fichiers partagés NFS 44
Figure III.3 : Installation NFS sur la Machine 2 44
Figure III.4 : Montage de système de fichiers 45
Figure III.5 : Test du système de fichiers NFS sur la Machine 1 46
Figure III.6 : Test du système de fichiers NFS sur la Machine 2 46
Figure III.7 : Installation ReaR 47
Figure III.8 : Création de système de secours et de sauvegarde 48
Figure III.9 : Contenu du fichier de récupération ReaR 49
Figure III.10 : Contenu du répertoire monté par NFS 49
Figure III.11 : Système endommagé 50
Figure III.12 : Copie du système dans un support de stockage 50
Figure III.13 : Importation de l'image ISO 51
Figure III.14 : Démarrage en mode BIOS 51
Figure III.15 : Sauvegarde de la configuration 52
Figure III.16 : Démarrage en mode secours ReaR 52
Figure III.17 : Lancer la reprise du système 53
Figure III.18 : Redémarrage de la MV 53
Figure III.19 : Redémarrage du Machine 1 54
Figure III.20 : Système récupéré 54

Liste des tableaux

Tableau I.1: Niveaux d'impact 16
Tableau I.2: Niveaux de probabilité 16
Tableau I.3: Evaluation qualitative 17
Tableau I.4: Risques classés selon une évaluation qualitative 18

Liste des annexes

Annexe 1 : Installation du logiciel NetBackup Master Server sous UNIX 63
Annexe 2: Configuration NetBackup Master Server 67
Annexe 3: Installation du logiciel NetBackup Media Server sous UNIX 69

Annexe 1 *: Installation du logiciel NetBackup Master Server sous UNIX*

Cette section décrit comment installer un nouveau NetBackup Master Server. Ces informations sont utilisées pour installer le logiciel serveur sur un ordinateur sans version existante de NetBackup.

Les instructions suivantes sont utilisées pour une installation de Master Server :

- Indiquer le Master Server ==> Indiquer le périphérique à utiliser comme Master Server et installer d'abord le logiciel de Master Server.
- Serveur EMM ==> Configuration du serveur EMM sur le Master Server. Tous les Master Servers doivent posséder leur propre configuration EMM.
- Achat de licences

Le serveur EMM (Enterprise Media Manager) : Contient des informations sur les médias, les robots et les lecteurs dans l'unité de stockage NetBackup Le courtier de ressources NetBackup interroge la base de données EMM pour allouer des unités de stockage, des lecteurs (y compris des chemins de lecteur) et des médias.

Pour installer le logiciel Master Server NetBackup :

1. Se connecter au serveur en tant que root.
2. Utiliser l'une des méthodes suivantes pour démarrer le script d'installation :
   - DVD :
     a. Insérer le DVD du serveur NetBackup pour la plate-forme appropriée dans le lecteur.
     b. Si nécessaire, monter le DVD.
     c. Entrer la commande suivante :

```
dvd_directory/install
```

Le **dvd_directory** est le chemin d'accès au répertoire dans lequel il est possible d'accéder au DVD.

   - Images ESD (fichiers téléchargés)
     a. Accéder à l'emplacement où résident les images d'installation
     b. Entrer la commande suivante :

```
./installer
```

3. Lorsque le message suivant s'affiche, appuyer sur **Entrée** pour continuer :

```
Veritas Installation Script
Copyright 1993 - 2016 Veritas Corporation, All Rights Reserved.


        Installing NetBackup Server Software


Please review the VERITAS SOFTWARE LICENSE AGREEMENT located on
the installation media before proceeding.  The agreement includes
details on the NetBackup Product Improvement Program.

For NetBackup installation and upgrade information specific to your
platform and to find out if your installed EEBs or hot fixes are
contained in this release, check out the Veritas Services and
Operations Readiness Tools (SORT) Installation and Upgrade
Checklist
and Hot fix and EEB Release Auditor, respectively, at
https://sort.veritas.com/netbackup.

ATTENTION!  To help ensure a successful upgrade to NetBackup 8.1.1,
please visit the NetBackup 8.x Upgrade Portal:
http://www.veritas.com/docs/000115678.

Do you wish to continue? [y,n] (y)
```

4. Lorsque le message suivant apparaît, appuyer sur **Entrée** pour continuer :

```
Is this host a master server? [y/n] (y)
```

5. Pour l'emplacement d'installation de NetBackup, entrer les informations de plate-forme appropriées comme suit :
   - Quand la question suivante apparaît, appuyer sur **Entrée** pour accepter la valeur par défaut (y) :

```
The NetBackup and Media Manager software is built
for use on <platform> hardware. Do you want to install
```

```
NetBackup and Media Manager files? [y,n] (y)
```

- Quand la question suivante apparaît, sélectionner où installer le logiciel de NetBackup et de Media Manager :

```
NetBackup and Media Manager are normally
installed in /usr/openv.
Is it OK to install in /usr/openv? [y,n] (y)
```

  - Le chemin d'accès affiché pour Solaris est **/opt/openv**.
  - Pour accepter le paramètre par défaut (y), appuyer sur **Entrée**.
  - Pour modifier l'emplacement d'installation, saisir (n) et appuyer sur **Entrée**. Entrer ensuite l'emplacement approprié.

6. Saisir la licence du serveur NetBackup ou Enterprise.
7. Taper (y), puis suivre les instructions qui s'affichent pour ajouter des clés de licence pour les autres options et agents NetBackup.
8. Confirmer ou entrer le nom d'ordinateur correct lorsque le message suivant s'affiche :

```
Installing NetBackup Enterprise Server version: 8.1.1
If this machine will be using a different network interface than
the default (name), the name of the preferred interface
should be used as the configured server name. If this machine
will be part of a cluster, the virtual name should be used as the
configured server name.
The domainname of your server appears to be "domain". You
may choose to use this domainname in your configured NetBackup
server name, or simply use "name" as the configured
NetBackup server name.
Would you like to use "name.domain" as the configured NetBackup
server name of this machine? [y, n] (y)
```

  - Pour accepter le nom affiché (par défaut), appuyer sur **Entrée**.
  - Pour modifier le nom affiché (par défaut), taper (n) et saisir le nom de votre choix.
  - Pour les serveurs NetBackup qui font partie d'un cluster, saisir le nom virtuel du serveur NetBackup plutôt que le nom réel de l'hôte local.

9. Identifier ou vérifier le serveur maître en répondant à la question suivante lorsqu'elle apparaît :

```
Is <name> the master server? [y, n] (y)
```

- Pour accepter le nom affiché (qui est le nom identifié à l'étape précédente), appuyer sur **Entrée**.
- Si un nom virtuel est assigné au serveur au cours de l'étape précédente, le script d'installation affiche la question suivante :

```
Is this server part of a cluster installation?
```

  - Si la réponse est oui, appuyer sur (y) et répondre à la série de questions de configuration de cluster qui s'affiche.
  - Si la réponse est non, appuyer sur (n).

10. Indiquer s'il existe des Media Serve pour ce Master Server en répondant à la question suivante lorsqu'elle s'affiche :

```
Do you want to add any media servers now? [y, n] (n)
```

11. Lorsque le message suivant apparaît, appuyer sur **Entrée** et accepter le nom par défaut du serveur EMM. Le serveur EMM doit être configuré sur le Master Server. Tous les Master Server doivent posséder leur propre configuration EMM.

```
NetBackup maintains a centralized catalog (separate from the
image catalog) for data related to media and device
configuration, device management, storage units, hosts and host
aliases, media server status, NDMP credentials, and other
information. This is managed by the Enterprise Media Manager
server.
Enter the name of the Enterprise Media Manager (default: <name>)
```

12. Répondre à la question suivante lorsqu'elle apparaît :

```
Do you want to start the NetBackup job-related processes so backups
and restores can be initiated? [y, n] (y)
```

13. Pour un Master Server NetBackup en cluster, répéter ces étapes sur chaque nœud dans lequel NetBackup doit être exécuté.
14. Une fois l'installation initiale terminée, il est possible d’installer tout autre produit NetBackup additionnel (tel qu'un package de langue).

Annexe 2: *Configuration NetBackup Master Server*

La procédure suivante est utilisée pour configurer le Master Server NetBackup :

1. Sur le Master Server, créer les politiques de sauvegarde NetBackup. Pour les listes de noms de client, utiliser les noms de client NetBackup (par exemple ; nbclient01) plutôt que les noms d'hôte de réseau dynamique (par exemple ; dynamic01).
2. Créer la base de données client sur le Master Server.

   La base de données client se compose de répertoires et de fichiers dans le répertoire suivant :

   - Sous Windows :

```
chemin_installation\NetBackup\db\client
```

   - Sous UNIX :

```
/usr/openv/netbackup/db/client
```

3. Créer, mettre à jour, répertorier et supprimer des entrées client avec la commande **bpclient**.

   La commande **bpclient** se trouve dans le répertoire suivant :

   - Sous Windows :

```
chemin_installation\NetBackup\bin\admincmd
```

   - Sous UNIX :

```
/usr/openv/netbackup/bin/admincmd
```

4. Pour voir ce qui se trouve actuellement dans la base de données client, exécuter **bpclient** comme suit :

   - Sous Windows :

```
chemin_installation\NetBackup\bin\admincmd\bpclient -L -All
```

   - Sous UNIX :

```
 /usr/openv/netbackup/bin/admincmd/bpclient -L -All
```

La sortie ressemble à ce qui suit :

```
Client Name: nbclient01
```

```
Current Host:
Hostname: *NULL*
IP Address: 0.0.0.0
Connect on non-reserved port: no
Dynamic Address : yes
.
.
.
Client Name: nbclient10
Current Host:
Hostname: *NULL*
IP Address: 0.0.0.0
Connect on non-reserved port: no
Dynamic Address : yes
```

Le client NetBackup informe le serveur NetBackup de son nom de client NetBackup et de son nom d'hôte réseau. Ensuite, les champs Hôte actuel, Nom d'hôte et Adresse IP affichent les valeurs pour ce client NetBackup.

Annexe 3: *Installation du logiciel NetBackup Media Server sous UNIX*

Cette section décrit comment installer un nouveau NetBackup Media Server. Utiliser ces informations pour installer le logiciel serveur sur un ordinateur sans version existante de NetBackup.

Le logiciel Media Server gère la robotique et les périphériques de stockage au sein d'environnement NetBackup.

Master Server et le logiciel du serveur EMM doivent être installé.

Utiliser les instructions suivantes pour une installation de Media Server :

- Indiquer le Media Server ==> Indiquer le périphérique à utiliser comme Media Server et installer d'abord le logiciel de Media Server.
- Serveur EMM ==> Le serveur EMM doit être installé et en cours d'exécution avant d'installer le logiciel du Media Server.
- Achat de licences

Le serveur EMM (Enterprise Media Manager) : Contient des informations sur les médias, les robots et les lecteurs dans l'unité de stockage NetBackup Le courtier de ressources NetBackup interroge la base de données EMM pour allouer des unités de stockage, des lecteurs (y compris des chemins de lecteur) et des médias.

Pour installer le logiciel Media Server NetBackup :

2. Se connecter au serveur en tant que root.
3. Utiliser l'une des méthodes suivantes pour démarrer le script d'installation :
    - DVD :
        a. Insérer le DVD du serveur NetBackup pour la plate-forme appropriée dans le lecteur.
        b. Si nécessaire, monter le DVD.
        c. Entrer la commande suivante :
        dvd_directory/install
        Le **dvd_directory** est le chemin d'accès au répertoire dans lequel il est possible d'accéder au DVD.
    - Images ESD (fichiers téléchargés)
        c. Accéder à l'emplacement où résident les images d'installation

d. Entrer la commande suivante :

./installer

4. Lorsque le message suivant s'affiche, appuyer sur **Entrée** pour continuer :

```
Veritas Installation Script
Copyright 1993 - 2016 Veritas Corporation, All Rights Reserved.


        Installing NetBackup Server Software


Please review the VERITAS SOFTWARE LICENSE AGREEMENT located on
the installation media before proceeding.  The agreement includes
details on the NetBackup Product Improvement Program.

For NetBackup installation and upgrade information specific to your
platform and to find out if your installed EEBs or hot fixes are
contained in this release, check out the Veritas Services and
Operations Readiness Tools (SORT) Installation and Upgrade
Checklist
and Hot fix and EEB Release Auditor, respectively, at
https://sort.veritas.com/netbackup.

ATTENTION!  To help ensure a successful upgrade to NetBackup 8.1,
please visit the NetBackup 8.x Upgrade Portal:
http://www.veritas.com/docs/000115678.

Do you wish to continue? [y,n] (y)
```

5. Indiquer si le périphérique est le Master Server en répondant à la question suivante lorsqu'elle apparaît :

```
Is this host the master server? [y,n] (n)
```

6. Vérifier ou entrer le nom d'ordinateur correct lorsque le message suivant s'affiche :

```
Installing NetBackup Enterprise Server version: 8.1
If this machine will be using a different network interface than
the default (name), the name of the preferred interface
should be used as the configured server name. If this machine
will be part of a cluster, the virtual name should be used as the
```

```
configured server name.
The domainname of your server appears to be "domain". You
may choose to use this domainname in your configured NetBackup
server name, or simply use "name" as the configured
NetBackup server name.
Would you like to use "name" as the configured NetBackup server
name of this machine? [y, n] (y)
```

7. Mentionner le nom du serveur maître lorsque cette question s'affiche :

```
What is the fully qualified name of the master server?
```

Si le serveur maître est en cluster, entrer le nom virtuel du serveur maître.

8. Pour l'emplacement d'installation de NetBackup, entrer les informations de plate-forme appropriées comme suit :
    - Lorsque la question suivante s'affiche, appuyer sur Entrée pour accepter la valeur par défaut (y).

```
The NetBackup and Media Manager software is built
for use on <platform> hardware. Do you want to install
NetBackup and Media Manager files? [y,n] (y)
```

    - Lorsque la question suivante s'affiche, sélectionner où installer les logiciels NetBackup et Media Manager :

```
NetBackup and Media Manager are normally
installed in /usr/openv.
Is it OK to install in /usr/openv? [y,n] (y)
```

        - Le chemin affiché pour Solaris est **/opt/openv**.
        - Pour accepter la valeur par défaut (y), appuyer sur **Entrée**.
        - Pour modifier l'emplacement d'installation, taper (n) et appuyer sur **Entrée**. Ensuite entrer la destination appropriée.

9. Une fois que l'emplacement d'installation des fichiers binaires est confirmé, le programme d'installation récupère les détails du certificat de l'autorité de certification.

```
Getting CA certificate details.
Depending on the network, this action may take a few minutes. To
continue without setting up secure communication, press Ctrl+C.
```

- L'action Ctrl+C entraine le relancement de l'installation ou la poursuite de l'installation sans les composants de sécurité requis. Si ces composants de sécurité sont absents, les sauvegardes et les restaurations peuvent échouer.

10. Vérifier les informations d'empreintes digitales et confirmer si elles sont exactes.

```
Master server [master_name] reports CA Certificate fingerprint
[fingerprint]. Is this correct? [y/n] (y)
Getting CA certificate details.
Depending on the network, this action may take a few minutes. To
continue without setting up secure communication, press Ctrl+C.
```

11. Une fois le certificat de l'autorité de certification stocké, le programme d'installation récupère le certificat de l'hôte

```
Getting host certificate.
Depending on the network, this action may take a few minutes. To
continue without setting up secure communication, press Ctrl+C.
```

- L'action Ctrl+C entraine le relancement de l'installation ou la poursuite de l'installation sans les composants de sécurité requis. Si ces composants de sécurité sont absents, les sauvegardes et les restaurations peuvent échouer.

12. Entrer la clé de licence **NetBackup Server** ou **NetBackup Enterprise Server**.
13. Taper (y), puis suivre les invites pour ajouter des clés de licence pour d'autres options et agents NetBackup. Bien qu'il soit possible d'ajouter des clés de licence ultérieurement, il est obligatoire de les saisir maintenant. Si des clés de licence vont être ajoutées ultérieurement via la console d'administration NetBackup-Java, la console doit être redémarrée.
14. Une fois toutes les clés de licence saisies, taper (q) pour quitter l'utilitaire de clé de licence et terminer l'installation du logiciel serveur.
15. Lorsque le message suivant s'affiche, appuyer sur **Entrée** et accepter le nom par défaut du serveur EMM. Le serveur EMM doit être configuré sur le Master Server. Tous les Master Servers doivent avoir leur propre configuration EMM.

```
Enter the name of the Enterprise Media Manager (default: <name>)
```

- Le nom du Master Server est affiché par défaut

16. Répéter les étapes 1 à 15 pour installer le logiciel du Media Server sur tous les Media Servers restants.