Université Abderrahmane Mira Béjaïa

Faculté des Sciences Exactes
Département Informatique

Mémoire de fin de Cycle

En vue de l'obtention du diplôme de Master Professionnel en Informatique

Option : Administration et Sécurité des Réseaux

Thème

Mise en place d'une solution de Disaster Recovery

Présenté par

Raid BAROUTDJI

Devant le jury composé de :

Présidente	Karima AIT ABDELOUHAB	MCB	Université de Bejaïa
Encadrant	Mohand YAZID	MCA	Université de Bejaïa
Examinatrice	Souhila MAMMERI	MAB	Université de Bejaia

Promotion : 2020 - 2021

Remerciements

Je tiens à exprimer toute ma reconnaissance à mon encadrant, Monsieur Mohand YAZID ainsi que Monsieur Omar LOUCHATI, Je les remercie de m'avoir encadré, orienté, aidé et conseillé.

Je désire aussi remercier les membres de jury d'avoir accepté de juger mon travail.

Mes vifs remerciements vont à ma très chère famille, ma mère, mon épouse, mes enfants, mes sœurs et leurs maris, ainsi que ma belle-famille, qui ont toujours été là pour moi. Je les remercie pour leurs encouragements et soutien.

Je voudrais exprimer ma reconnaissance envers Réda CHAFFAI, pour son aide, conseil et soutien, et envers Kenza BENCHALAL, pour avoir relu et corrigé mon mémoire, ses conseils de rédaction ont été très précieux, sans oublier mes amis et collègues de Tchin-Lait spa qui m'ont apporté leur soutien moral et intellectuel tout au long de ma démarche.

À toute personne qui a contribué de près ou de loin à la réalisation de ce travail, je présente mes remerciements, mon respect et ma gratitude.

Raid,

Dédicaces

A
Ma mère,
Mon épouse,
Mes enfants,
Je dédie ce modeste travail.

Raíd,

Table des Matières

Table des Matières iii

Liste des Abréviations v

Liste des Figures vi

Liste des Tableaux viii

Introduction Générale 1

Chapitre I : Notions de Base : Réseau Informatique, VPN, Virtualisation. 4

1. Introduction 4
2. Réseau Informatique 4
3. VPN 4
4. Virtualisation 4
5. Conclusion 5

Chapitre II : Présentation de l'environnement 6

1. Introduction 6
2. L'environnement de travail 6
3. Détails des infrastructures 6
4. Adressage IP 9
5. Problématique 10
6. Solution Proposée 10
7. Conclusion 10

Chapitre III : Présentation de la solution proposée (RecoverPoint For Virtual Machine) 11

1. Introduction 11
2. Présentation 11
3. Avantages 12
4. Point Dans le Temps (PiT) 12
5. Protection Locale et Distante pour les machines virtuelles 13
6. Composants de RecoverPoint for VM 14
   - *6.1. Virtual RecoverPoint Appliance (vRPA)* 14
   - *6.2. vRPA Cluster* 14
   - *6.3. RecoverPoint for VM Plug-in* 14
   - *6.4. RecoverPoint for VM Splitter* 14
   - *6.5. RecoverPoint for VM system* 14

7. Conclusion 14
Chapitre IV : Réalisation 16
1. Introduction 16
2. Préparation de l'infrastructure 16
2.1. Prérequis pour le déploiement de vRAP 16
2.2. Préparation du Réseau pour vRPA Cluster 16
2.3. Noms et configuration IP de la solution RecoverPoint for VM 17
2.4. Organisation de l'infrastructure virtuelle 18
2.5. Organisation des commutateurs virtuels (Distributed vSwitches) 18
3. Déploiement de RecoverPoint for VM 18
3.1. Création du port group pour le Data Traffic 18
3.2. Connexion des nœuds au Port Group Créé 19
3.3. Déploiement de vRPA 21
3.4. Déploiement du Plugin Server 26
3.5. Configuration du Cluster vRPA 26
4. Protection d'une VM 33
5. Test de basculement 38
6. Conclusion 43
Conclusion Générale et Perspectives 45
Annexe A : Netwrix Auditor 47
Annexe B : Centreon Monitoring 49
Références Bibliographiques 50

Liste des Abréviations

CG	**C**onsistency **G**roup
DHCP	**D**ynamic **H**ost **C**onfiguration **P**rotocol
DNS	**D**omain **N**ame **S**ystem
ESXi	**E**lastic **S**ky **X** **i**ntegrated (Hyperviseur de VMware)
IP	**I**nternet **P**rotocol
HCI	**H**yper-**C**onverged **I**nfrastructure
HTML	**H**yper**T**ext **M**arkup **L**anguage
MPLS	**M**ulti**P**rotocol **L**abel **S**witching
OVF	**O**pen **V**irtualization **F**ormat
PC	**P**ersonal **C**omputer
PG	**P**ort **G**roup
RDM	**R**aw **D**evice **M**apping
RDP	**R**emote **D**esktop **P**rotocol
RP	**R**ecover **P**oint
RPO	**R**ecovery **P**oint **O**bjective
RTO	**R**ecovery **T**ime **O**bjective
PiT	**P**oint-**i**n-**T**ime
VLT	**V**irtual **L**ink **T**runk
VM	**V**irtual **M**achine
VMDK	**V**irtual **M**achine **D**is**K**
VPN	**V**irtual **P**rivate **N**etwork
vRPA	**v**irtual **R**ecover **P**oint **A**ppliance
vSAN	**V**irtual **S**torage **A**rea **N**etwork
WAN	**W**ide **A**rea **N**etwork

Liste des Figures

Figure 1 - Réplication de VMs 3
Figure 2 - Vue de face de VxRail P570 7
Figure 3 - Vue arrière de VxRail P570 7
Figure 4 - Connexion des switches Dell avec le reste du réseau 8
Figure 5 - Connexion des nœuds aux switches (site de Setif) 8
Figure 6 - Protection locale et distante 13
Figure 7 - Création d'un Port Group pour vRPA 18
Figure 8 - Configuration du Port Group 19
Figure 9 – Ajout du nœud au Port Group créé 19
Figure 10 – Configuration de l'adresse IP du nœud 20
Figure 11 – Validation de la configuration 20
Figure 12 – Déploiement de l'appliance vRPA à partir d'un modèle OVF 21
Figure 13 - Choix du fichier OVF 21
Figure 14 – Configuration du nom de l'appliance vRPA 22
Figure 15 - Choix des ressources à utiliser par l'appliance vRPA 22
Figure 16 - Vérification des informations de l'appliance vRPA 23
Figure 17 - Contrat de licence de vRPA 23
Figure 18 - Configuration de l'appliance vRPA 24
Figure 19 - Sélection de stockage pour l'appliance vRPA 24
Figure 20 - Configuration réseau de l'appliance vRPA 25
Figure 21 - Configuration IP de l'appliance vRPA 25
Figure 22 - Validation de la configuration de vRPA 26
Figure 23 - Création d'un cluster vRPA à partir d'une appliance. 27
Figure 24 - Authentification dans vCenter. 27
Figure 25 - Configuration de l'environnement du cluster. 28
Figure 26 - Ajouts des appliances vRPA au cluster. 28
Figure 27 - Configuration réseau du cluster 29
Figure 28 - Configuration réseau du cluster - suite. 29
Figure 29 - Validation de la configuration. 30
Figure 30 - Connexion des deux clusters vRPA 31
Figure 31 - Définition de l'adresse IP du cluster distant 31
Figure 32 - Les deux clusters sont désormais connectés. 32
Figure 33 - RecoverPoint for VMs est accessible à partir du vCenter 32
Figure 34 - Propriétés de poste de travail DSI-O3 33
Figure 35 - Test de ping du serveur na-server à partir du poste client. 33
Figure 36 - Enregistrement DNS du serveur na-server 34
Figure 37 - Connexion en RDP au serveur na-server à partir du poste client. 34
Figure 38 - Protection de la VM à l'aide de RecoverPoint. 35
Figure 39 - Création d'une copie distante 35
Figure 40 - Accès à RecoverPoint à partir de vCenter. 36

Figure 41 - La copie est créée. 36
Figure 42 - Configuration de l'IP distante de la VM. 37
Figure 43 - Définir le réseau distant sur lequel la VM sera connectée. 37
Figure 44 - Initialisation de la copie. 38
Figure 45 - La copie est prête sur le cluster distant. 38
Figure 46 - Accès à RecoverPoint à partir du cluster distant 39
Figure 47 - Test d'une copie de VM. 39
Figure 48 - Démarrage de la copie dans un réseau de test. 40
Figure 49 – Lancement d'un Failover sur une copie de VM. 40
Figure 50 - La VM copie est allumée est connectée au réseau de production. 41
Figure 51 - Réplication de la VM dans le sens inverse. 42
Figure 52 - Enregistrement DNS corrigé sur le serveur DNS. 42
Figure 53 - Test de ping du serveur na-server à partir du poste client. 43
Figure 54 - Connexion en RDP au serveur na-server à partir du poste client. 43
Figure 55 - Netwrix Auditor. 47
Figure 56 - Risk Assessment - Netwrix Auditor 48
Figure 57 - Centreon Monitoring. 49

Liste des Tableaux

Tableau 1 - Adresses IP des équipements du site principal 9
Tableau 2 - Adresses IP des équipements du site distant 10
Tableau 3 - Configuration requise sur la plateforme virtuelle VMware..... 16
Tableau 4 - Ressources nécessaires par vRPA 16
Tableau 5 - Configuration IP de la solution RP for VM sur le site principal..... 17
Tableau 6 - Configuration IP de la solution RP for VM sur le site de secours..... 17
Tableau 7 - La structure de vRPA Cluster 18
Tableau 8 - Organisation des trafics selon les types 18

Introduction Générale

Dans le monde actuel et moderne, l'informatique est présente dans tous les détails de notre vie quotidienne, la plupart de nos gestes quotidiens, sont gérés par un ordinateur ou un logiciel à travers nos assistants quotidiens comme les smartphones et les tablettes.

Dans certains organismes et entreprises modernes, rien ne fonctionne sans faire appel à une ressource informatique, commençant par la rédaction d'une simple note de service, arrivant à la gestion d'une ligne de production ou un entrepôt de stockage complètement automatisée, tout en passant par la communication quotidienne, la gestion des projets et contrôle d'accès basé sur l'authentification biométrique.

Toutes ces opérations quotidiennes que nous venons de citer, sont gérées par des terminaux (ordinateurs ou autres) et traitées et stockées sur des serveurs, ces derniers peuvent être présents sur place, à distance ou en cloud.

Depuis plusieurs années déjà, le terme « virtualisation » est beaucoup utilisé lorsqu'on parle de serveurs, en d'autres termes, on ne parle plus de serveurs physiques, plutôt que de serveurs virtuels.

La virtualisation est un concept qui consiste à transformer une machine physique en plusieurs machines virtuelles, c'est-à-dire, plusieurs entités logicielles qui simulent des serveurs, sont hébergées sur un même serveur physique, et qui partagent et exploitent les ressources physiques de ce dernier.

L'avantage de cette technologie est la flexibilité dans l'utilisation des serveurs et applications installées, elle permet aussi de diminuer les coûts.

D'un autre côté, les moyens de communication existants depuis quelques années, ont transformé le monde en un petit village, désormais, n'importe quel individu peut communiquer avec d'autres personnes en utilisant différentes solutions existantes.

Dans le monde professionnel, les organismes qui possèdent des différents sites éloignés physiquement, recourent à l'utilisation de *VPN (Virtual Private Network)* pour interconnecter ces sites, cette technologie consiste à utiliser un

réseau publique tel que Internet pour créer une liaison virtuelle entre deux réseaux distants, à travers un tunnel chiffré en utilisant des protocoles prédéfinis.

Par exemple, un employé d'une entreprise dont le bureau est à Bejaia, accède à une donnée sur un serveur local qu'il pense qu'il est hébergé dans le data center à côté de son bureau, mais ce serveur en réalité se trouvent dans un data center à Alger, où les deux data centers sont reliés par une liaison VPN pour former un seul réseau privé.

La protection de toutes ces données que nous venons de citer est très importante si on veut assurer une continuité des services.

Il existe plusieurs façons pour protéger les données informatiques, commençant par les solutions de cyber sécurité et firewalling pour empêcher tout accès non autorisé ou mal intentionné à ces données, jusqu'à la sauvegarde de ces données pour pouvoir les récupérer suite à une perte causée par une attaque ou un sinistre.

Ce travail propose une solution de protection de données basée sur la réplication des machines virtuelles critiques, en temps réel, sur un site distant relié au site principal par une liaison VPN MPLS (MultiProtocol Label Switching), comme le montre la figure 1.

En cas d'arrêt d'une VM (Virtual Machine) sur le site principal, une copie distante de cette VM peut être lancée, et les utilisateurs peuvent continuer à travailler sans sentir une différence, grâce à la correction des enregistrements DNS (**D**omain **N**ame **S**ystem) au moment du *Failover*.

Dans le cas d'un arrêt total du data center principal à la suite d'une catastrophe naturelle, le data center de secours sera lancé, on parle ici d'un *Disaster Recovery*.

Une connaissance préalable de la plateforme de virtualisation VMware est nécessaire pour réaliser ce travail.

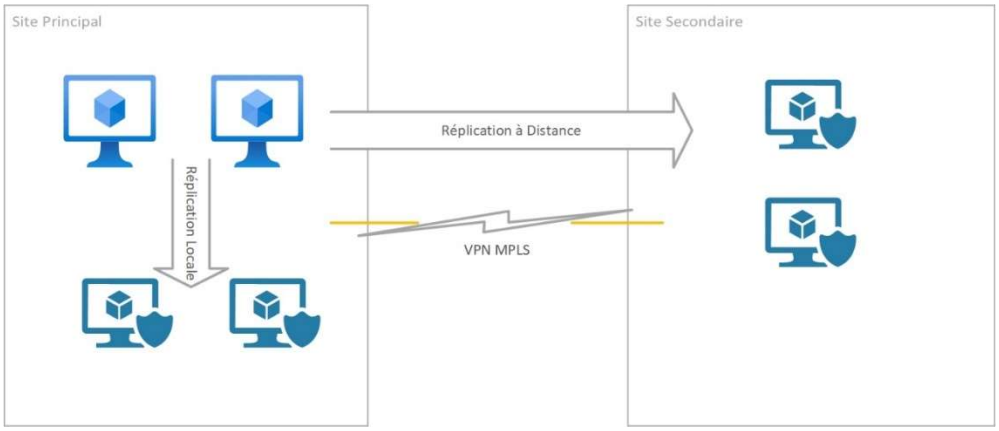


Figure 1 - Réplication de VMs

Ce mémoire de master est structuré de la manière suivante :

Dans le premier chapitre, nous présenterons d'une façon très brève les notions de base des réseaux informatiques, du VPN ainsi que la virtualisation. Vu que beaucoup de travaux traitent ces définitions, nous avons préféré de ne pas trop les détailler et de consacrer une plus grande partie de ce mémoire à la réalisation du projet.

Dans le deuxième chapitre, nous présenterons l'environnement du travail utilisé pour réaliser notre projet, nous parlerons de l'infrastructure physique existante ainsi que la solution de virtualisation utilisée à savoir VMware, nous évoquerons aussi le problème de protection des données et nous proposerons une solution.

Le troisième chapitre sera consacré à la présentation en détails de la solution proposée à savoir RecoverPoint du constructeur américain Dell-EMC. Nous parlerons de la façon dont cette solution protège les données et nous préciserons le rôle de chaque composant.

Dans le quatrième et dernier chapitre, nous détaillerons les étapes suivies pour mettre en place et configurer la solution, nous allons voir aussi dans un exemple réel comment protéger une VM en la dupliquant sur un site distant et comment récupérer cette VM en la lançant à partir du site distant après l'avoir arrêtée sur le site principal.

Enfin, nous terminons ce travail par une conclusion générale et quelques perspectives.

Chapitre I : Notions de Base : Réseau Informatique, VPN, Virtualisation.

1. Introduction

Dans ce chapitre, nous présenterons d'une façon très brève les notions de base des réseaux informatiques, du VPN ainsi que la virtualisation. Nous avons préféré de ne pas trop détailler ces définitions et de consacrer une plus grande partie de ce mémoire à la réalisation du projet. Enfin, nous terminons ce chapitre par une conclusion.

2. Réseau Informatique

"Un réseau est un moyen de communication qui permet à des individus ou des groupes de partager des informations et des services.

La technologie des réseaux informatiques constitue l'ensemble des outils qui permettent à des ordinateurs de partager des informations et des ressources" [1].

Un réseau informatique est composé de plusieurs équipements appelés nœuds, ces nœuds communiquent entre eux en utilisant des protocoles bien spécifiques.

3. VPN

"VPN, pour Virtual Private Network (réseau privé virtuel) désigne un réseau crypté dans le réseau Internet, qui permet à une société dont les locaux seraient géographiquement dispersés de communiquer et partager des documents de manière complètement sécurisée, comme s'il n'y avait qu'un local avec un réseau interne" [2].

Un réseau VPN repose sur un protocole appelé « protocole de tunneling ». Ce protocole permet de faire circuler les informations de l'entreprise de façon cryptée d'un bout à l'autre du tunnel. Ainsi, les utilisateurs ont l'impression de se connecter directement sur le réseau de leur entreprise [3].

4. Virtualisation

La virtualisation s'appuie sur des logiciels pour simuler une fonctionnalité matérielle et créer un système informatique virtuel. Ce modèle permet aux services informatiques d'exécuter plusieurs systèmes virtuels (et plusieurs systèmes d'exploitation et applications) sur un seul et même serveur. Cela se traduit par des économies d'échelle et des gains d'efficacité.

“La virtualisation des serveurs, ou « server virtualization », est le processus qui consiste à diviser un serveur physique en plusieurs serveurs virtuels uniques et isolés au moyen d’une application logicielle. Chaque serveur virtuel peut exécuter indépendamment ses propres systèmes d’exploitation” [3].

5. Conclusion

Dans ce chapitre, nous nous sommes intéressés à la définition des notions de base sur quelques éléments importants dans la réalisation de notre travail, tel que la virtualisation et le VPN.

Chapitre II : Présentation de l'environnement

1. Introduction

Dans ce chapitre, nous allons présenter l'environnement utilisé pour réaliser ce travail, l'infrastructure existante en détail, ainsi que le problème de protection des données, et la solution proposée.

2. L'environnement de travail

Notre environnement de travail est composé de deux sites distants reliés entre eux par une liaison VPN. Chaque site est composé de :

- Réseau local ;
- Une connexion Internet ;
- Un Data Center ;
- Des ordinateurs (postes utilisateurs) ;
- Des Serveurs ;
- Des imprimantes et d'autre équipements réseau.

Les deux réseaux locaux sont interconnectés par une liaison VPN MPLS en partenariat avec **Algérie Télécom**.

Nous acceptons que l'un des sites est situé physiquement à Bejaia (Site principal) et l'autre est situé à Sétif (Site secondaire et site de secours).

Les utilisateurs des deux sites accèdent en utilisant leurs PCs (soit en local ou via la liaison VPN) à des applications métiers qui s'exécutent sur des serveurs hébergés dans le data center principal (Bejaia).

Notre travail consiste à répliquer les serveurs importants hébergés dans le site principal vers le site de secours pour pouvoir les exploiter (à partir du site de secours) en cas de problème empêchant leur fonctionnement au niveau du site principal.

3. Détails des infrastructures

Chaque site possède une infrastructure hyperconvergée (HCI), cette dernière est composée de plusieurs serveurs physiques Dell-EMC (Voir les figures 2 et 3), sur lesquels nous avons installé VMware vSphere, ces serveurs sont gérés par VMware vCenter comme un seul serveur physique.

Les disques durs de ces serveurs physiques forment un vSAN (Virtual Storage Area Network) qui est exploité par vCenter comme un espace de stockage commun.

Depuis longtemps, VxRail est le produit phare lorsque on parle de vSAN.

Infrastructure du site principal (Bejaia) est composée de :

- 05 nœuds Dell-EMC VxRail P570F (Hyperviseur ESXi) ;
- Deux switches Dell S4128f-ON.

Infrastructure du site secondaire (Setif) est composée de :

- 04 nœuds Dell-EMC VxRail P570 (Hyperviseur ESXi) ;
- Deux switches Dell S4128f-ON.

Figure 2 - Vue de face de VxRail P570

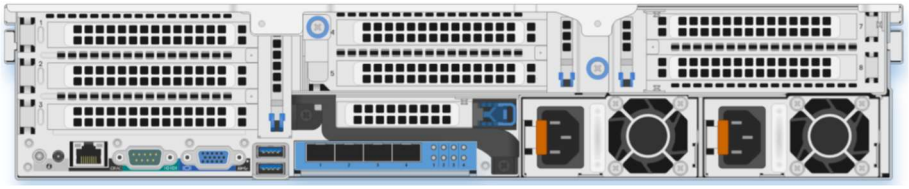


Figure 3 - Vue arrière de VxRail P570

Chaque nœud est connecté aux deux switches avec 4 liaisons optiques de 10Gb chacune (deux liaisons entre chaque nœud et un switch), les deux switches sont connectés au reste du réseau local à l'aide de 4 liaisons optiques aussi (deux liaisons pour chaque switch) comme illustré dans la figure 5, en plus, les deux switches sont interconnectés à l'aide de deux liaisons optiques de 100Gb chacune à travers des ports VLT (Virtual Link Trunk) comme illustré dans la figure 4.

Cette topologie offre une connexion optimale et très tolérante aux pannes.

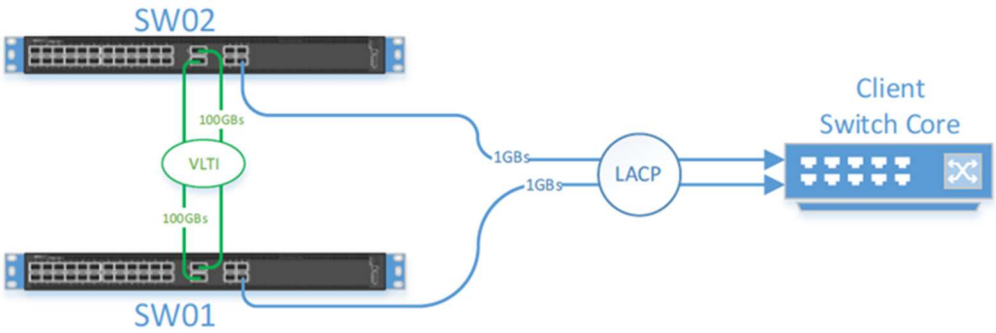


Figure 4 - Connexion des switches Dell avec le reste du réseau

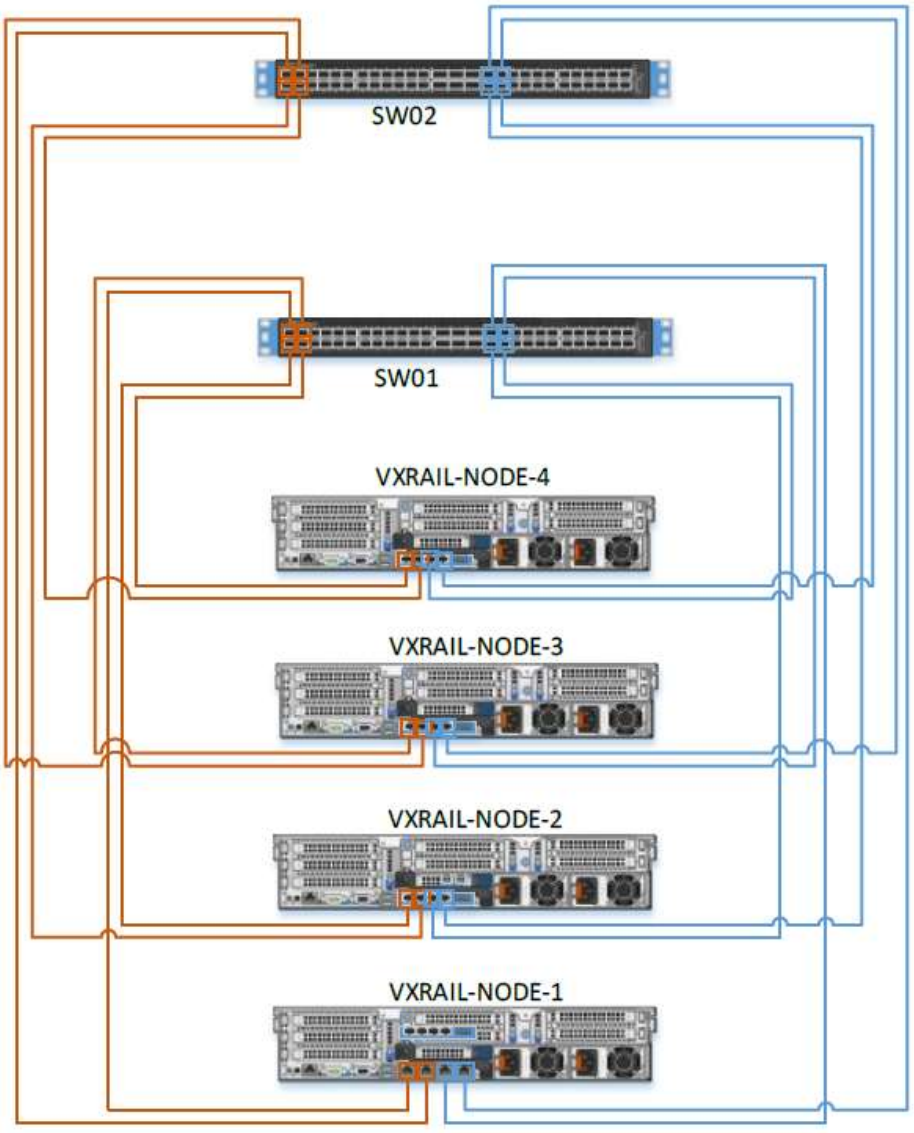


Figure 5 - Connexion des nœuds aux switches (site de Setif)

Dans la réalisation de notre travail, nous nous intéressons à deux autres machines à savoir :

1. Un serveur **na-server** : c'est un serveur virtuel qui héberge l'application Netwrix Auditor qui est un outil d'audit qui permet d'assurer un suivi des activités dans les environnements informatiques, tel que les modifications effectuées au niveau d'Active Directory par exemple, d'une façon simple et facile. Ce serveur est situé au niveau du Data Center du site principal, il sera dupliqué vers le site de secours, nous allons essayer de reprendre les services de ce serveur sur le site de secours après qu'il est arrêté sur le site principal.
2. Un poste utilisateur **DSI-03** : c'est une machine virtuelle exécutant Windows 11, qui sera utilisée pour tester l'accès au serveur na-server sur le site principal, et puis sur le site de secours.

De plus, chaque site possède un ou plusieurs serveurs contrôleurs de domaines, DNS et DHCP (Dynamic Host Configuration Protocol) pour assurer un bon fonctionnement de l'infrastructure.

4. Adressage IP

Les adresses IP utilisées dans le site principal sont énumérées dans le Tableau 1 :

- Les serveurs sont configurés dans le sous réseau : 192.168.1.0/24 ;
- Les postes utilisateurs sont configurés dans le sous réseau : 10.10.8.0/24 ;
- Les nœuds VxRail sont configurés dans le sous réseau 10.10.51.0/24.

Network	IP	Host Name
Management Network 10.10.51.0/24	10.10.51.1	vx-esxi-01
	10.10.51.2	vx-esxi-02
	10.10.51.3	vx-esxi-03
	10.10.51.4	vx-esxi-04
	10.10.51.5	vx-esxi-05
Servers Network 192.168.1.0/24	192.168.1.70	na-server
	192.168.1.2	dc-bejaia
	192.168.1.100	dc-02-bejaia
User Network 10.10.8.0/24	10.10.8.133	DSI-03

Tableau 1 - Adresses IP des équipements du site principal

Les adresses IP utilisées dans le site secondaire sont énumérées dans le Tableau 2 :

- Les serveurs sont configurés dans le sous réseau : 192.168.4.0/24 ;
- Les nœuds VxRail sont configurés dans le sous réseau 10.40.51.0/24.

Network	IP	Host Name
Management Network 10.40.51.0/24	10.40.51.1	vx-esxi-stf-01
	10.40.51.2	vx-esxi-stf-02

	10.40.51.3	vx-esxi-stf-03
	10.40.51.4	vx-esxi-stf-04
Servers Network 192.168.4.0/24	192.168.4.2	dc-setif

Tableau 2 - Adresses IP des équipements du site distant

5. Problématique

Les serveurs hébergés sur un data center et qui offrent des services à des utilisateurs peuvent s'arrêter de fonctionner à la suite de plusieurs facteurs, par exemple :

- Panne de la machine virtuelle ;
- Panne du serveur physique hébergeant la VM ;
- Panne électrique au data center qui va provoquer l'arrêt des serveurs ;
- Coupure du réseau informatique entre le data center et les postes utilisateurs ;
- Une catastrophe naturelle qui va toucher le data center et le rendre hors service.

Dans ces cas-là, il faut trouver une solution de protection des données qui va nous permettre la reprise des services rapidement.

6. Solution Proposée

Pour résoudre le problème cité dans la section précédente, nous proposons la solution Dell EMC RecoverPoint® for Virtual Machines, cette solution protège les données en répliquant les serveurs d'un site à un autre, et permet de reprendre le service d'un serveur donné au cas où ce dernier n'est plus fonctionnel sur le premier site, ou si le site est complètement inaccessible à la suite d'une catastrophe naturelle par exemple, tout cela, d'une façon transparente à l'utilisateur final.

Cette solution sera présentée en détail dans le chapitre prochain.

7. Conclusion

Dans ce chapitre, nous avons présenté l'environnement utilisé pour effectuer notre travail. L'environnement est composé de deux réseaux locaux distants (deux sites éloignés géographiquement) qui sont liés via une liaison VPN MPLS, où les données d'un site sont dupliquées sur l'autre site pour pourvoir reprendre les services sur le site de secours en cas d'incident sur le site principal.

Chapitre III : Présentation de la solution proposée (RecoverPoint For Virtual Machine)

1. Introduction

Ce chapitre présente la solution RecoverPoint for Virtual machine, qui sert à la protection des données en les dupliquant en local ou sur un site distant.

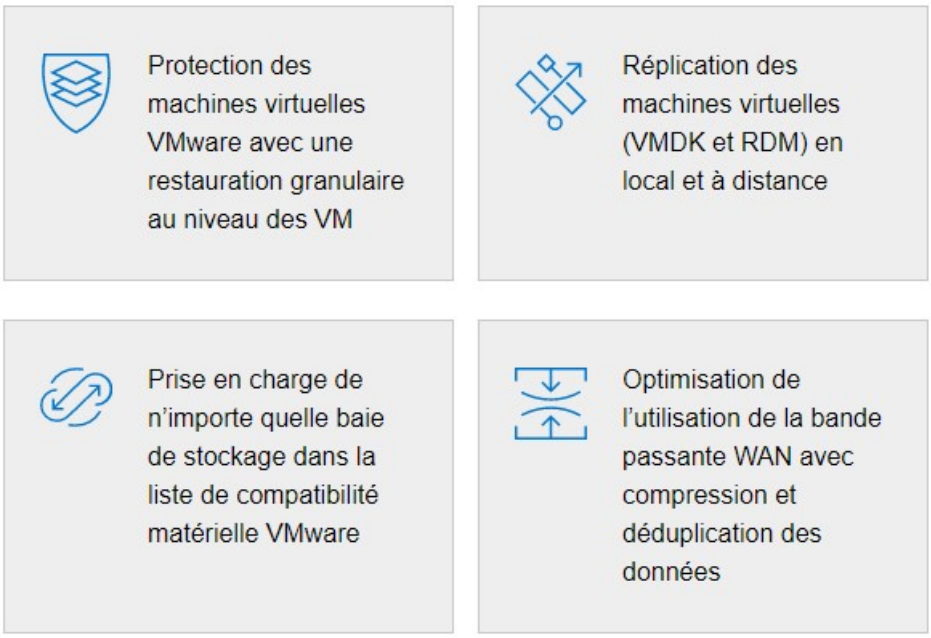
2. Présentation

Dell EMC RecoverPoint® for Virtual Machines redéfinit la protection des données pour les environnements virtualisés VMware. Il assure une protection granulaire au niveau des machines virtuelles, la réplication en local et à distance permettant d'effectuer une restauration sur site, à n'importe quel point dans le temps.

La solution prend en charge la réplication synchrone et asynchrone sur n'importe quelle distance avec une utilisation efficace de la bande passante WAN (Wide Area Network), réduisant fortement les coûts du réseau.

RecoverPoint for VMs simplifie la reprise après sinistre, le test de reprise après sinistre et la reprise des opérations grâce à des capacités intégrées d'orchestration et d'automatisation, accessibles directement à partir de VMware vCenter.

La solution fournit un workflow de reprise après sinistre automatisé, fiable et reproductible qui accroît l'efficacité opérationnelle de restauration et de protection des données des utilisateurs.



3. Avantages

- Protège les machines virtuelles VMware avec une granularité au niveau des VM ;
- Les administrateurs travaillent depuis VMware vCenter via un plug-in ;
- Récupération en cas de sinistre avec des RPO (Recovery Point Objective) d'une durée inférieure à 15 minutes ;
- Prend en charge tous les types de stockage et d'application ;
- Permet la protection continue des données pour la récupération *PiT* sur site pour RPO et RTO (Recovery Time Objective) quasi nuls ;
- Cohérence des restaurations pour les applications interdépendantes ;
- Stratégies de réplication synchrones ou asynchrones ;
- Protège les données à l'aide de groupes de cohérence (CG) propriétaires et d'ensembles de groupes de cohérence, assurant la cohérence de la récupération pour une application ou des applications interdépendantes ;
- Prise en charge multisite avec au maximum une réplication Fan-in 4:1 pour le site de reprise centralisé protégeant plusieurs filiales et une réplication Fan-out 1:4 pour les opérations de développement et de test ;
- Prend en charge des environnements vSphere, y compris vSphere 6.7U1 et vSAN 6.7U1.

4. Point Dans le Temps (PiT)

Grâce à son intégration étroite avec VMware, RecoverPoint for Virtual Machines protège les machines virtuelles avec une granularité au niveau des machines virtuelles.

Son plug-in vCenter permet aux administrateurs de : protéger une ou plusieurs machines virtuelles en local ou à distance sur le site cible ; effectuer la découverte automatisée, le provisionnement et l'orchestration pour le test de récupération en cas de sinistre ; basculement et restauration automatique vers n'importe quel PiT ; et orchestration de performance avancée (par exemple, séquençage de mise sous tension de machine virtuelle).

En exploitant les groupes de cohérence et les jeux de groupes de cohérence, les administrateurs peuvent effectuer avec cohérence une PiT sur l'ensemble des applications interdépendantes réparties sur les clusters VMware ESX.

Les entreprises peuvent par exemple bénéficier de cette puissante fonction pour restaurer avec exactitude le fonctionnement d'un processus de transactions commerciales de bout en bout couvrant le système de commandes, les opérations

de paiement, la gestion du stock et la gestion de la chaîne logistique, tous déployés dans des machines virtuelles.

Pour récupérer n'importe quel PiT, RecoverPoint for Virtual Machines utilise la consignation pour conserver les informations à un point dans le temps concernant toutes les modifications apportées aux données protégées.

Le temps de restauration le plus court au dernier point dans le temps, retour en arrière jusqu'à un point dans le temps, RPO court à n'importe quel point dans le temps permettant une restauration en quelques secondes seulement avant toute corruption des données, correction de l'erreur.

5. Protection Locale et Distante pour les machines virtuelles

Pour notre cas, la solution RecoverPoint for VM sera déployée sur les deux sites : Le site de production « Bejaia » et le site de secours « Sétif ».

Avec RecoverPoint for VM on peut avoir une protection en local et/ou une protection distante (Remote) comme illustré dans la figure 6.

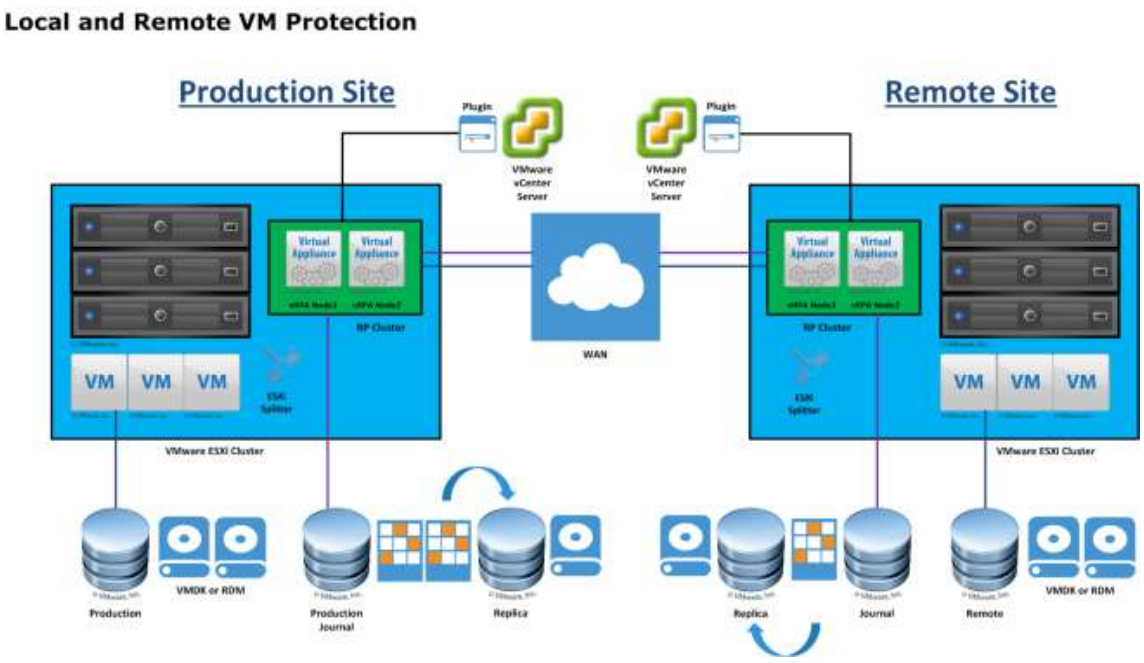


Figure 6 - Protection locale et distante

En effet, RecoverPoint for VMs permet aux utilisateurs de répliquer des machines virtuelles simplement et facilement et de gérer la réplication des machines virtuelles à partir de vSphere Web Client à l'aide du plug-in RecoverPoint. Les utilisateurs peuvent également utiliser les fonctions RecoverPoint telles que l'accès à un point dans le temps, le basculement sur incident, les tests, etc.

6. Composants de RecoverPoint for VM

Les composants de RecoverPoint for VM sont :

6.1. Virtual RecoverPoint Appliance (vRPA)

Les RecoverPoint Appliance sont des appliances virtuelles qui gèrent la réplication des machines virtuelles. Les vRPA sont déployées en utilisant vSphere Web client à partir de vCenter.

6.2. vRPA Cluster

Le cluster vRPA est composé de deux à huit vRPAs qui travaillent ensemble pour protéger et répliquer les VM, le cluster sera créé et les vRPAs seront connectées ensemble en utilisant le RecoverPoint for VM Deployer Wizard.

6.3. RecoverPoint for VM Plug-in

C'est un plugin HTML5 qui sera déployé dans vSphere Web Client User Interface après la création du cluster vRPA. Il permet aux administrateurs d'utiliser la solution à partir de l'interface web de vSphere.

6.4. RecoverPoint for VM Splitter

C'est un software propriétaire (EMC) installé sur chaque ESXi faisant partie d'un cluster ESXi impliqué dans une RecoverPoint for VM Replication ou sur lesquels tourne une vRPA.

Le splitter repère chaque écriture sur le VMDK et envoie une copie a une vRPA puis au volume de stockage.

Le splitter est automatiquement installé sur ESXi après l'enregistrement du cluster ESXi au niveau de vRPA cluster.

6.5. RecoverPoint for VM system

Est constitué d'un ou plusieurs vRPA cluster, comme suit :

- Un vRPA cluster : pour une protection locale uniquement ;
- Deux vRPA cluster ou plus : pour une protection locale et distante.

7. Conclusion

Dans ce troisième chapitre, nous avons présenté la solution Dell EMC RecoverPoint® for Virtual Machines, et comment elle protège les données dans les environnement virtualisés VMware. Nous avons détaillé les avantages de cette solution tels que la protection granulaire au niveau de VM.

Nous avons détaillé aussi quelques notions telles que le Point dans le Temps et nous avons vu la possibilité de protéger une VM en local ou à distance.

En fin, nous avons présenté les différents composants de la solution.

Chapitre IV : Réalisation

1. Introduction

Dans ce chapitre, nous allons voir les étapes à suivre pour mettre en place la solution Dell EMC RecoverPoint® for Virtual Machines, sa configuration ainsi que la reprise de service d'un serveur sur le site de secours après l'avoir arrêté sur le site principal.

2. Préparation de l'infrastructure

La première étape à suivre est de mettre en place les appliances vRPA et de créer les clusters vRPA (un cluster par site).

2.1. Prérequis pour le déploiement de vRAP

Le Tableau 3 décrit la configuration requise sur la plateforme virtuelle VMware

DESCRIPTION	EXIGENCE
Dell EMC RECOVERPOINT FOR VIRTUAL MACHINES	5.2.1
SERVEURS VMWARE VCENTER ET ESX (FOURNIS PAR LE CLIENT)	Versions 6.0U2, 6.5 et 6.7U1 avec client Web vCenter vSphere
VSAN	VSAN 6.0 et 6.5 6.6, 6.7U1
INFRASTRUCTURE RÉSEAU (FOURNIE PAR LE CLIENT)	Configuration de réseau flexible avec entre 1 et 4 réseaux virtuels

Tableau 3 - Configuration requise sur la plateforme virtuelle VMware

Le Tableau 4 montre les ressources nécessaires par vRPA

CPU VIRTUELS	MEMOIRE	DISQUE
2 CPU virtuels/4 GHz	8 Go	35 Go
4 CPU virtuels/8 GHz	8 Go	35 Go
8 CPU virtuels/16 GHz	8 Go	35 Go

Tableau 4 - Ressources nécessaires par vRPA

2.2. Préparation du Réseau pour vRPA Cluster

Pour que le serveur ESXi communique avec les vRPA, plusieurs adaptateurs réseau logiciel sur chaque serveur ESXi qui exécutera les vRPA ou les machines virtuelles protégées peuvent être utilisés.

Un seul port VMkernel est requis, cependant, les bonnes pratiques consistent à en configurer deux.

Dans notre cas la configuration est comme suite :

- 01 VMK pour chaque ESXi dans le réseau de management qui va accueillir le flux de management et de réplication (utilisation du Port Group de management existant).
- 01 VMK (DATA) pour chaque ESXi dédié pour la communication entre les ESXi et les vRPA (sera créé avant le déploiement de vRPA).

2.3. Noms et configuration IP de la solution RecoverPoint for VM

Site principal:
(voir Tableau 5)

Network	IP	Host Name
Management Network 10.10.51.0/24	10.10.51.1	vx-esxi-01
	10.10.51.2	vx-esxi-02
	10.10.51.3	vx-esxi-03
	10.10.51.4	vx-esxi-04
	10.10.51.5	vx-esxi-05
	10.10.51.21	vrpa01 (WAN + LAN)
	10.10.51.22	vrpa02 (WAN + LAN)
	10.10.51.20	vrpa-cluster
	10.10.51.23	vx-ps (vRPA plugin server)
VM Network (Data) 10.10.81.0/24	10.10.81.1	vx-esxi-01
	10.10.81.2	vx-esxi-02
	10.10.81.3	vx-esxi-03
	10.10.81.4	vx-esxi-04
	10.10.81.5	vx-esxi-05
	10.10.81.21	vrpa01 (Data Traffic)
	10.10.81.22	vrpa02 (Data Traffic)

Tableau 5 - Configuration IP de la solution RP for VM sur le site principal

Site de secours :
(Voir Tableau 6)

Network	IP	Host Name
Management Network 10.40.51.0/24	10.40.51.1	vx-esxi-stf-01
	10.40.51.2	vx-esxi-stf-02
	10.40.51.3	vx-esxi-stf-03
	10.40.51.4	vx-esxi-stf-04
	10.40.51.5	vx-esxi-stf-05
	10.40.51.21	vrpa01-stf (WAN + LAN)
	10.40.51.22	vrpa02-stf (WAN + LAN)
	10.40.51.20	vrpa-cluster-stf
	10.40.51.23	vx-ps-stf (vRPA plugin server)
VM Network (Data) 10.40.81.0/24	10.40.81.1	vx-esxi-stf-01
	10.40.81.2	vx-esxi-stf-02
	10.40.81.3	vx-esxi-stf-03
	10.40.81.4	vx-esxi-stf-04
	10.40.81.5	vx-esxi-stf-05
	10.40.81.21	vrpa01-stf (Data Traffic)
	10.40.81.22	vrpa02-stf (Data Traffic)

Tableau 6 - Configuration IP de la solution RP for VM sur le site de secours

2.4. Organisation de l'infrastructure virtuelle

Le Tableau 7 résume la structure de vRPA Cluster

Site	Cluster	vRPA
Principal	vrpa-cluster	vrpa01, vrpa02
Secondaire	vrpa-cluster-stf	vrpa01-stf, vrpa02-stf

Tableau 7 - La structure de vRPA Cluster

2.5. Organisation des commutateurs virtuels (Distributed vSwitches)

Les 4 ports SFP+ 10GBs vont accueillir les différents trafics de la plateforme hyper convergée VxRail.

Sur le tableau 8 on peut voir que chaque type de Traffic est active sur un uplink et en mode standby sur un autre cela permet de séparer pour mieux répartir la charge et éviter les goulots d'étranglements et aussi assure un uplink de secours dans le cas d'une panne sur un uplink,

Ci-dessous l'organisation des trafics selon les types :

Traffic Type	Uplink1	Uplink2	Uplink3	Uplink4
Management	Unused	Unused	Active	Standby
vSAN	Standby	Active	Unused	Unused
vRPA-Data Traffic	Unused	Unused	Active	Standby

Tableau 8 - Organisation des trafics selon les types

3. Déploiement de RecoverPoint for VM

3.1. Création du port group pour le Data Traffic

Dans vSphere Web Client, et dans la partie Réseau, nous allons créer un nouveau Port Group appelé vRPA_PG (voir les figures de 7 jusqu'à 11) :

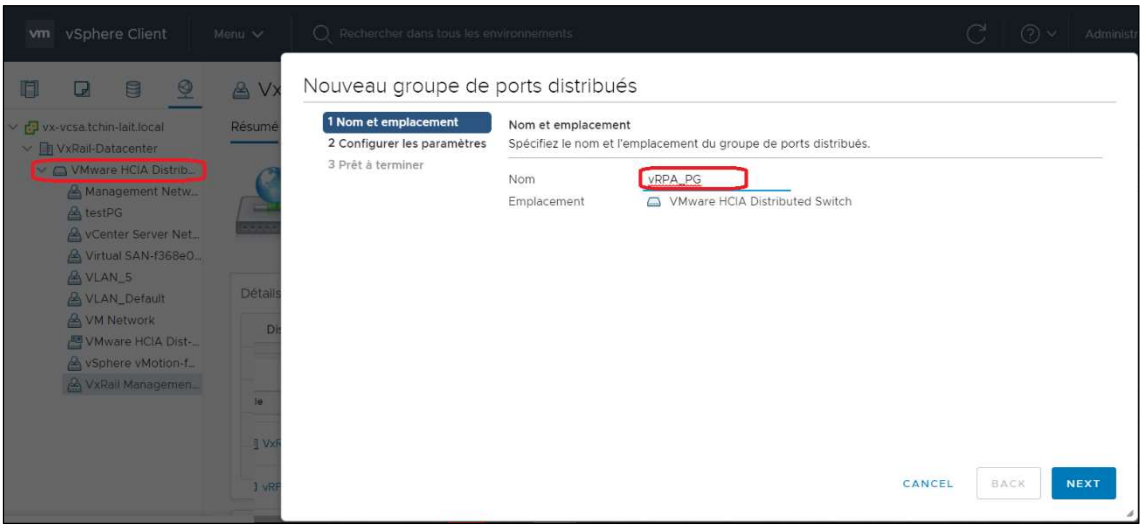


Figure 7 - Création d'un Port Group pour vRPA

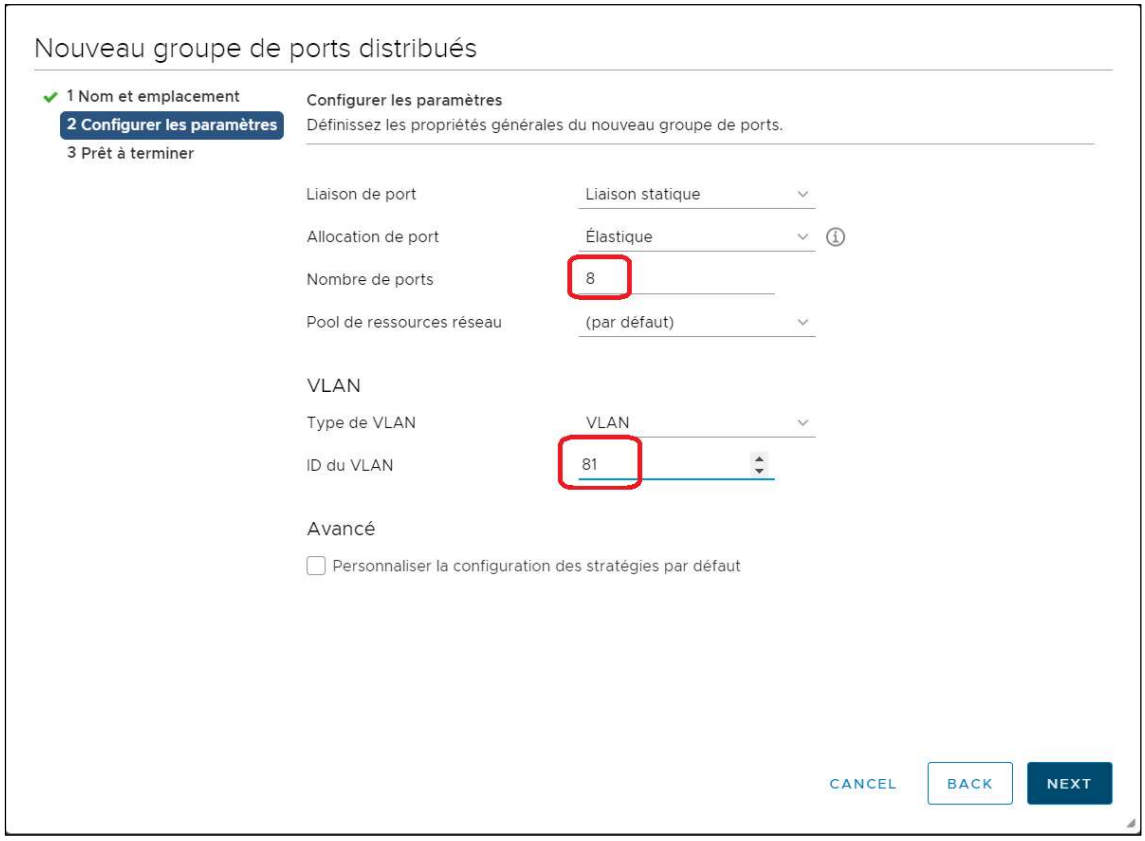


Figure 8 - Configuration du Port Group

3.2. Connexion des nœuds au Port Group Créé

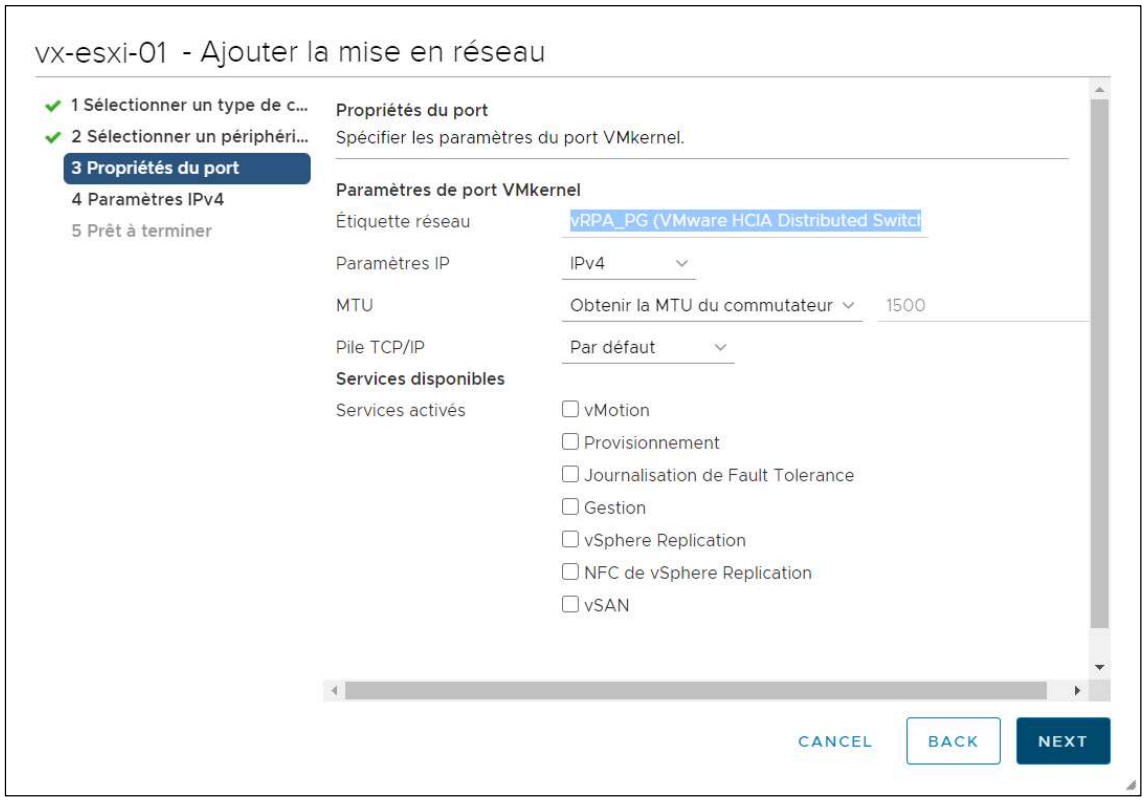


Figure 9 – Ajout du nœud au Port Group créé

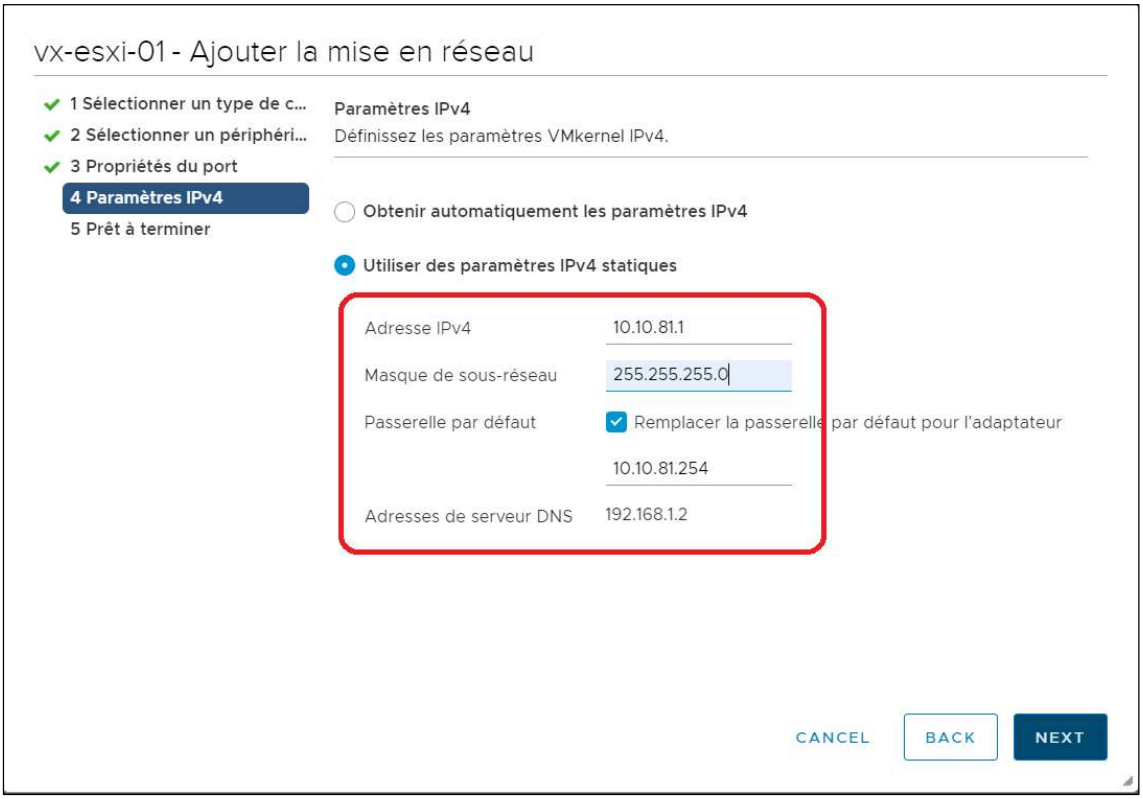


Figure 10 – Configuration de l'adresse IP du nœud

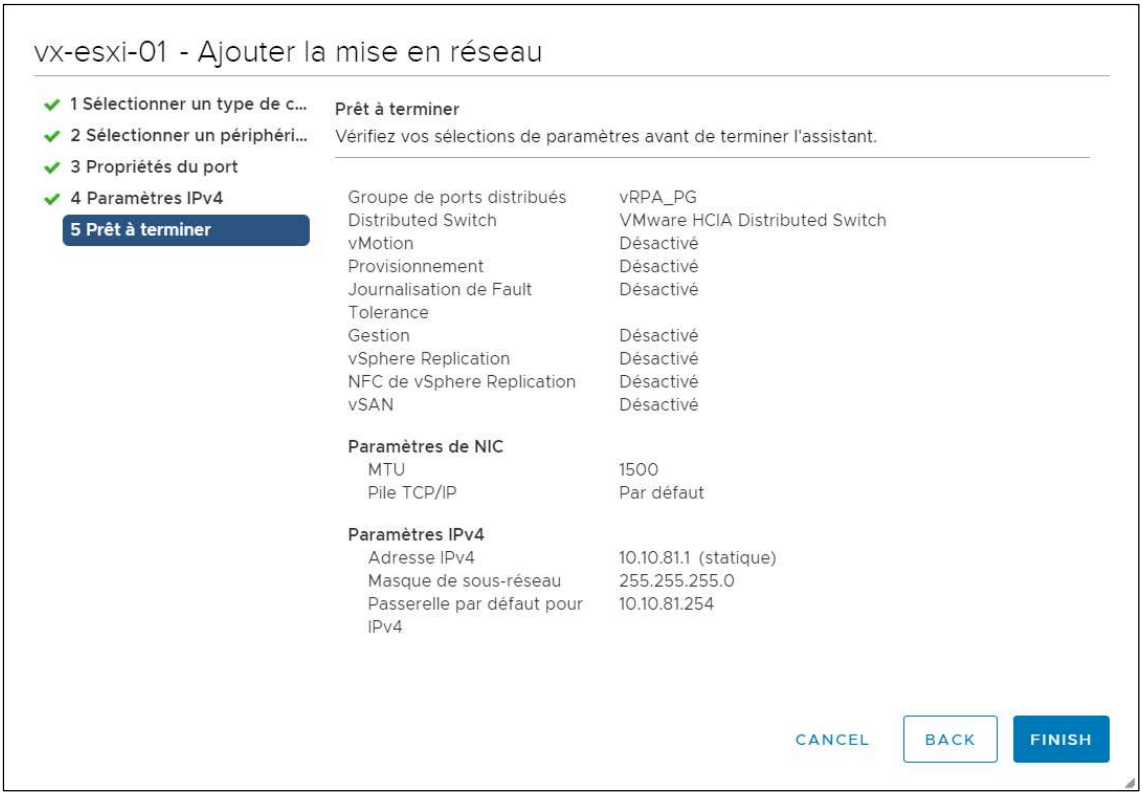


Figure 11 – Validation de la configuration

Nous avons répété l'opération sur tous les nœuds ESXi des deux sites (Bejaia et Setif).

3.3. Déploiement de vRPA

Les appliances vRPA sont disponibles en téléchargement sur http://support.emc.com, sous forme d'images OVF (Open Virtualization Format). Après l'avoir téléchargée, on va créer directement une nouvelle VM à partir du modèle OVF (voir les figures de 12 jusqu'à 22) :

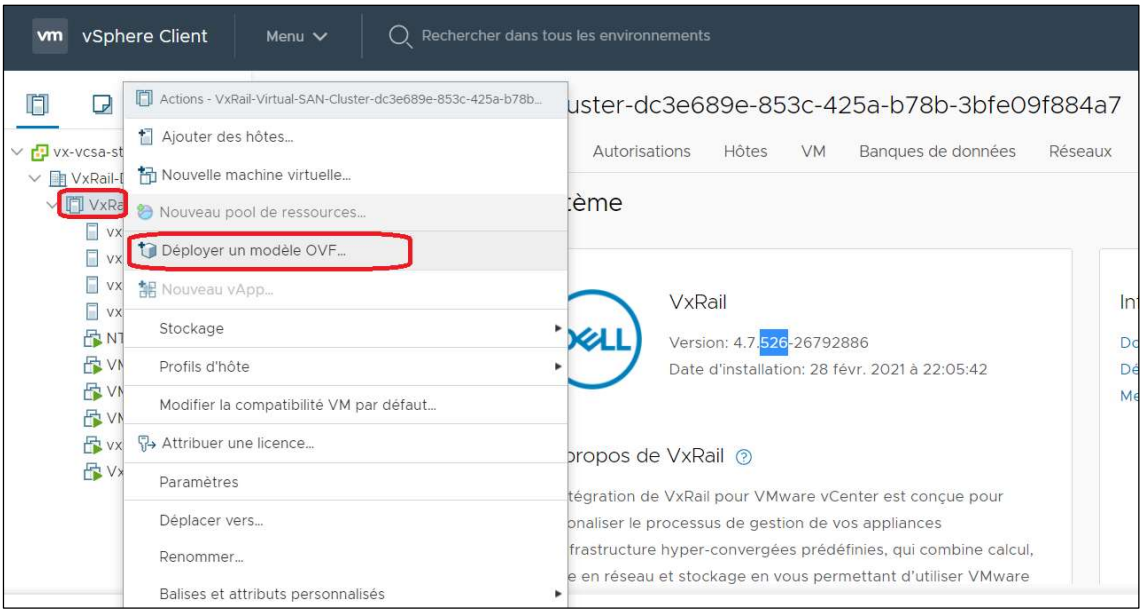


Figure 12 – Déploiement de l'appliance vRPA à partir d'un modèle OVF

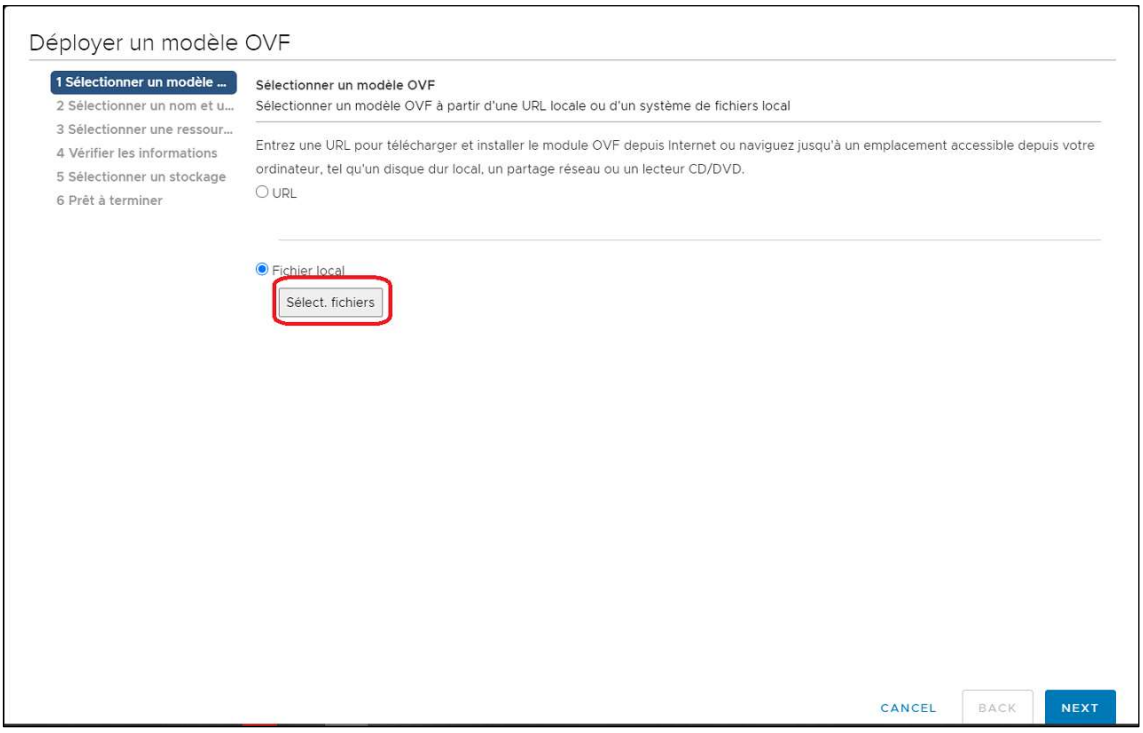


Figure 13 - Choix du fichier OVF

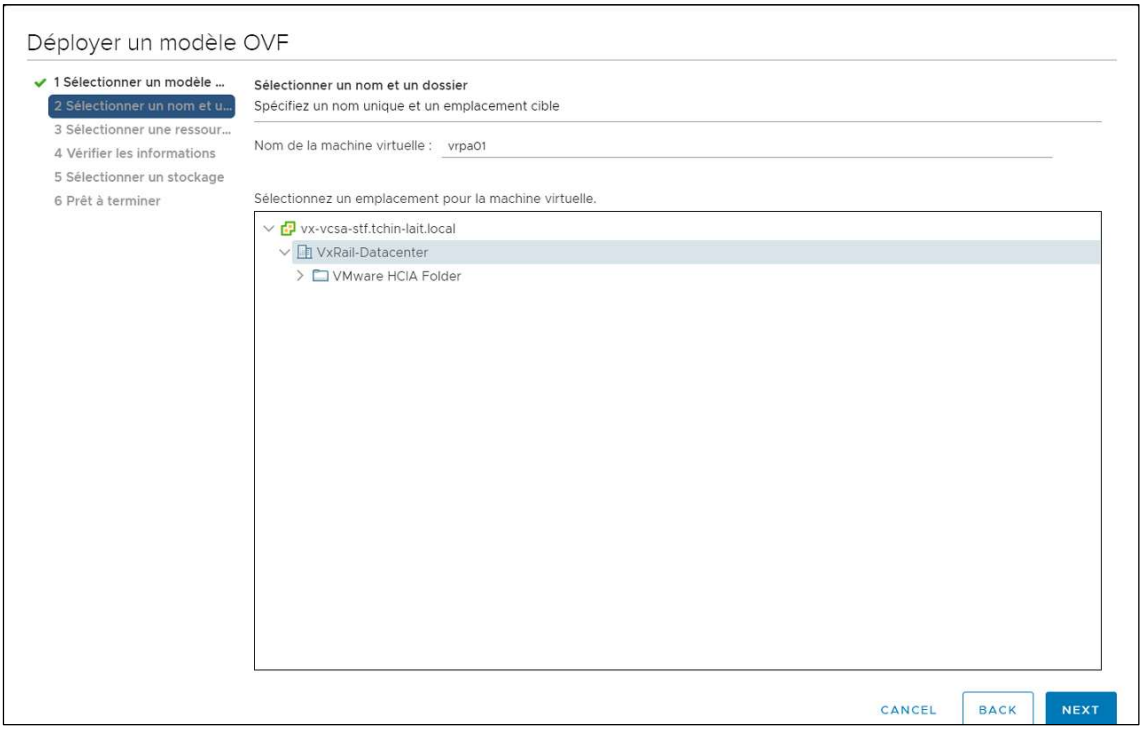


Figure 14 – Configuration du nom de l'appliance vRPA

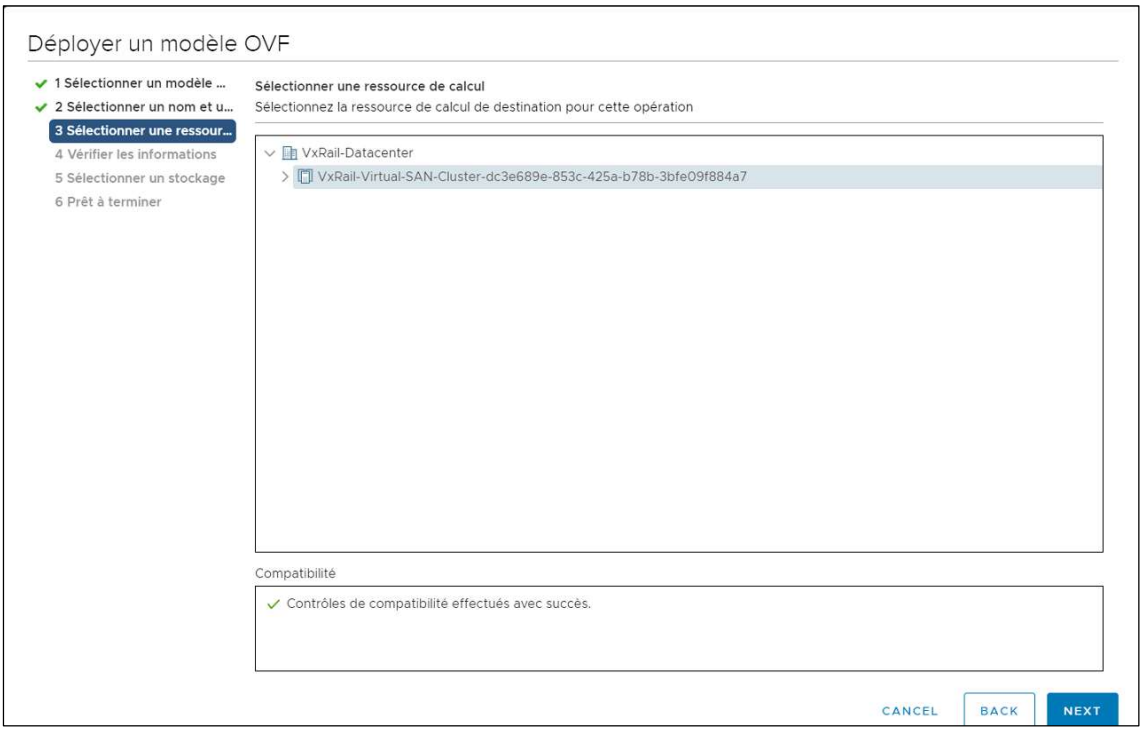


Figure 15 - Choix des ressources à utiliser par l'appliance vRPA

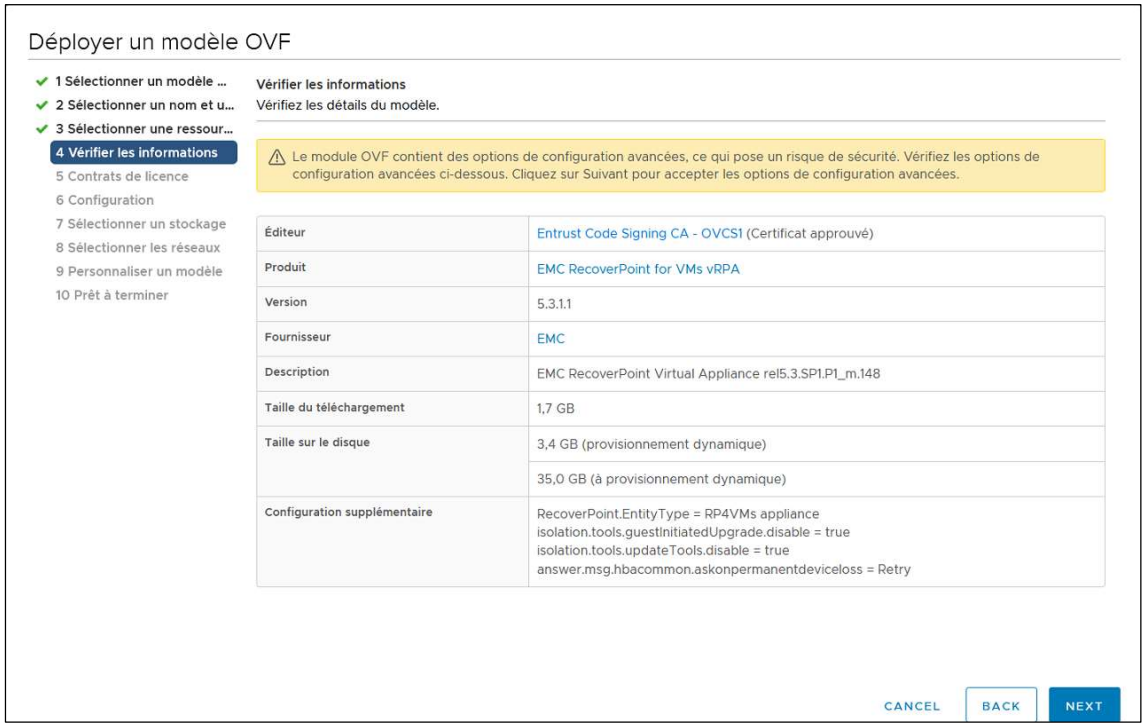


Figure 16 - Vérification des informations de l'appliance vRPA

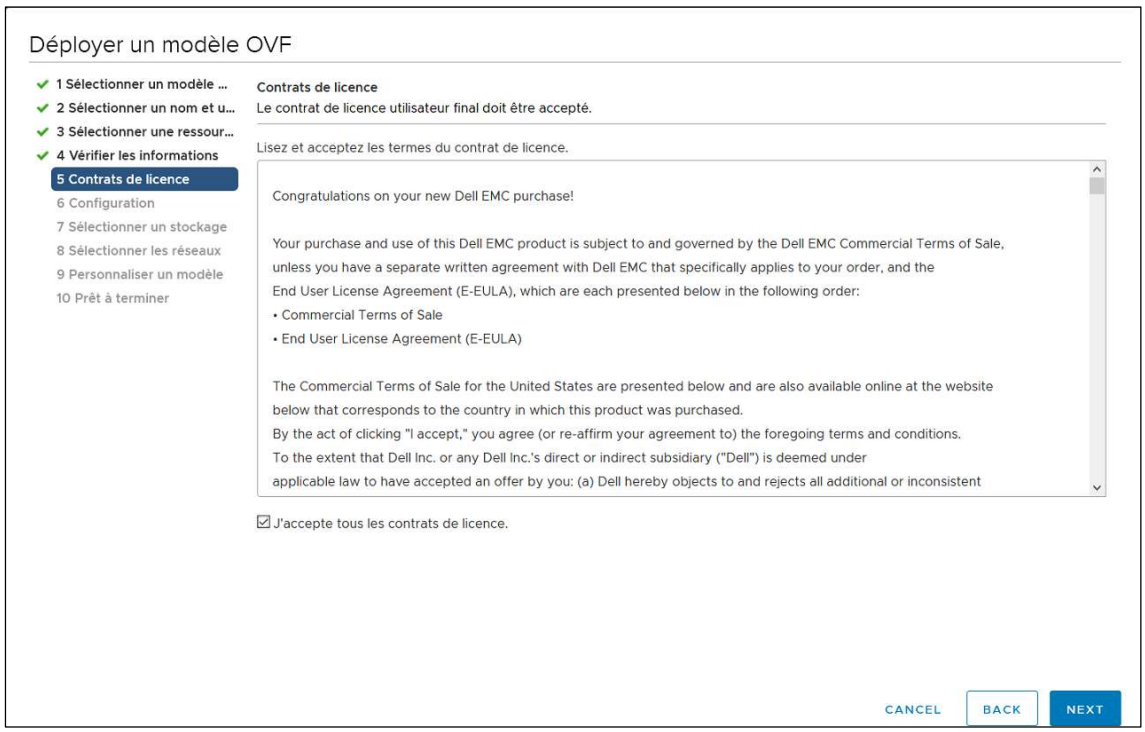


Figure 17 - Contrat de licence de vRPA

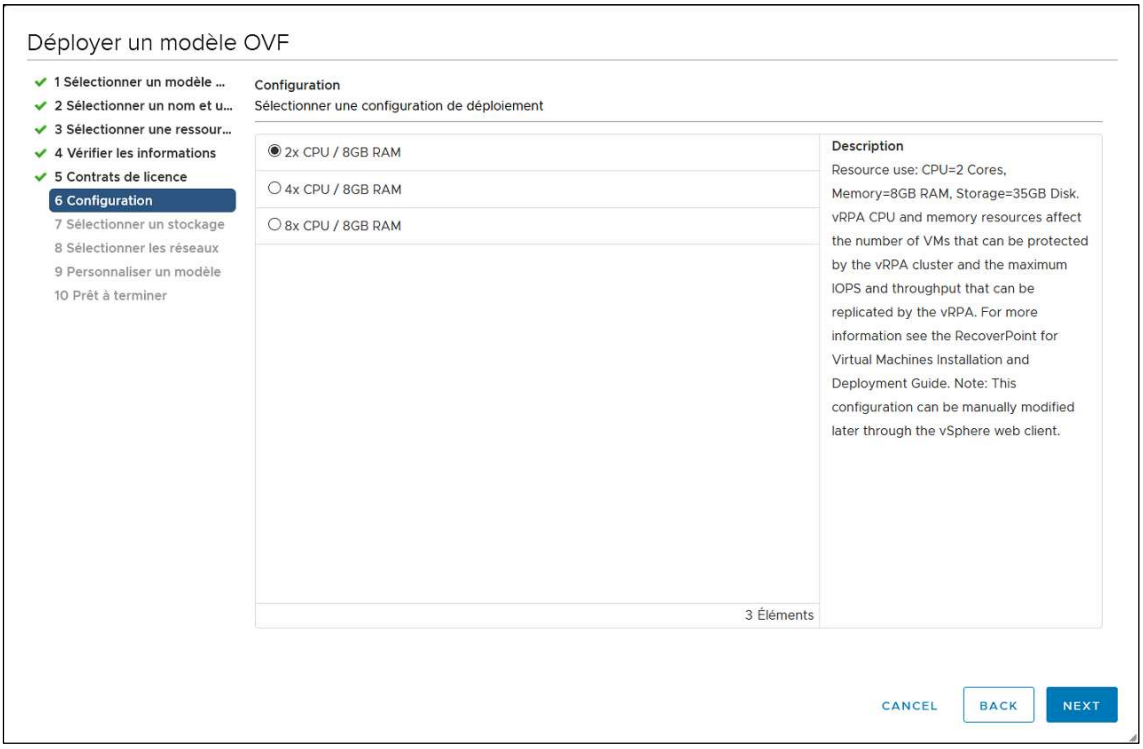


Figure 18 - Configuration de l'appliance vRPA

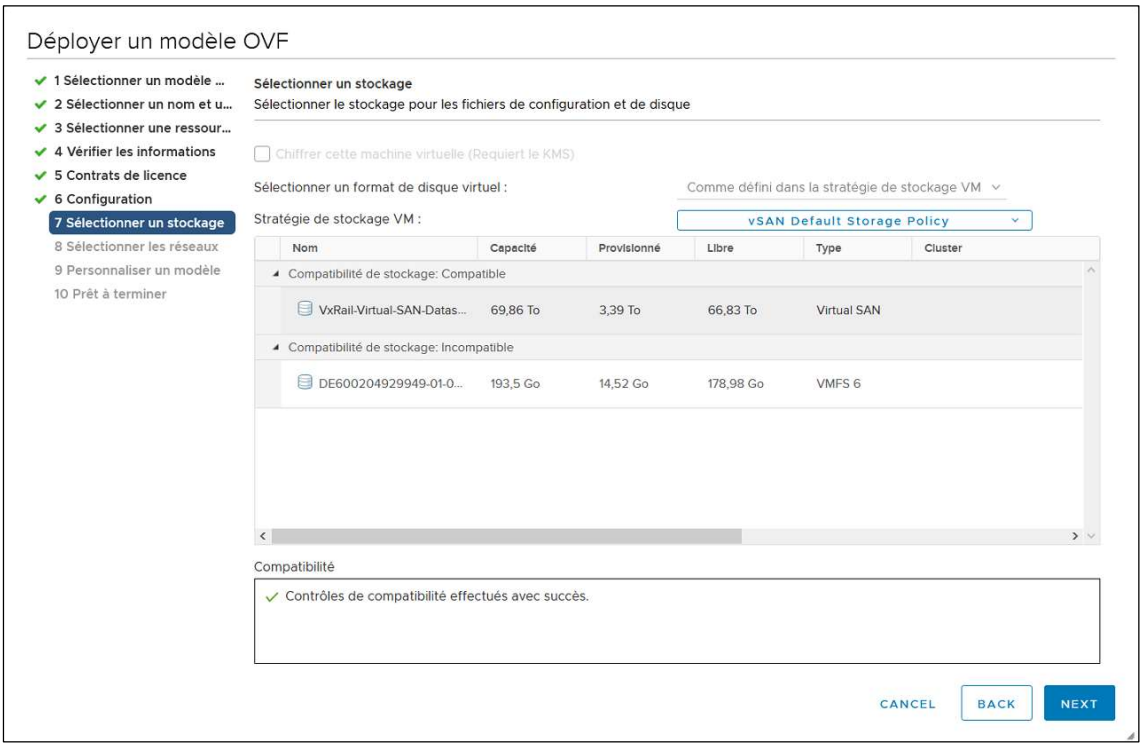


Figure 19 - Sélection de stockage pour l'appliance vRPA

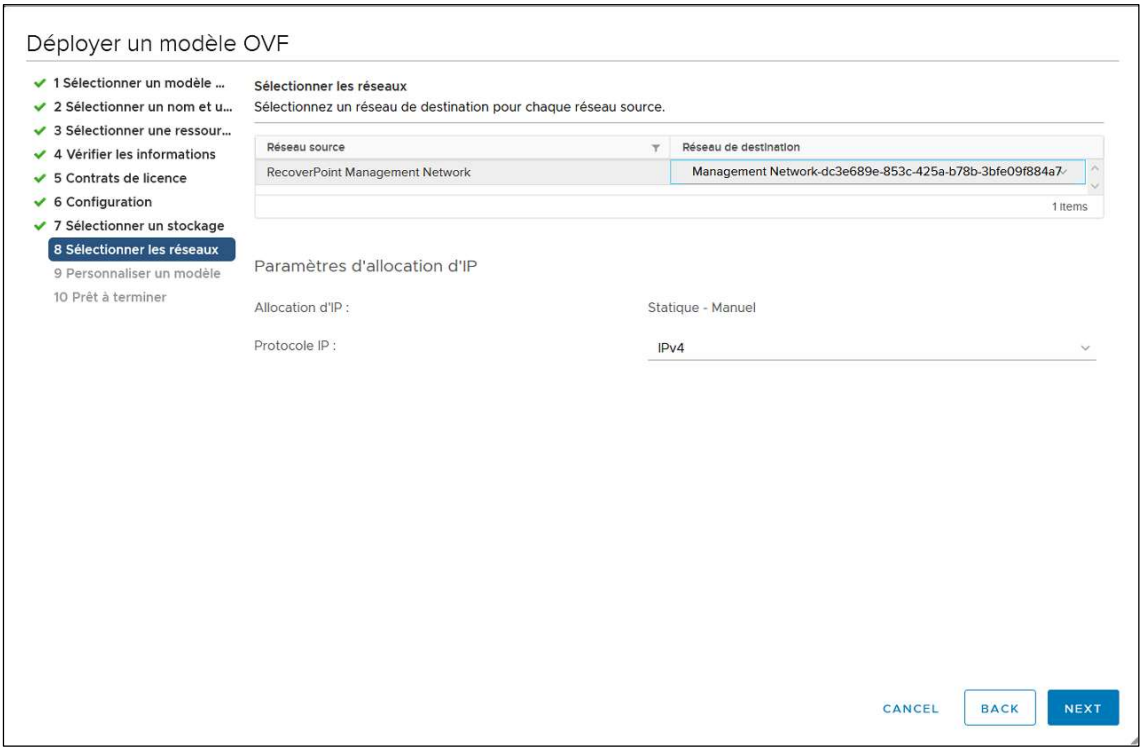


Figure 20 - Configuration réseau de l'appliance vRPA

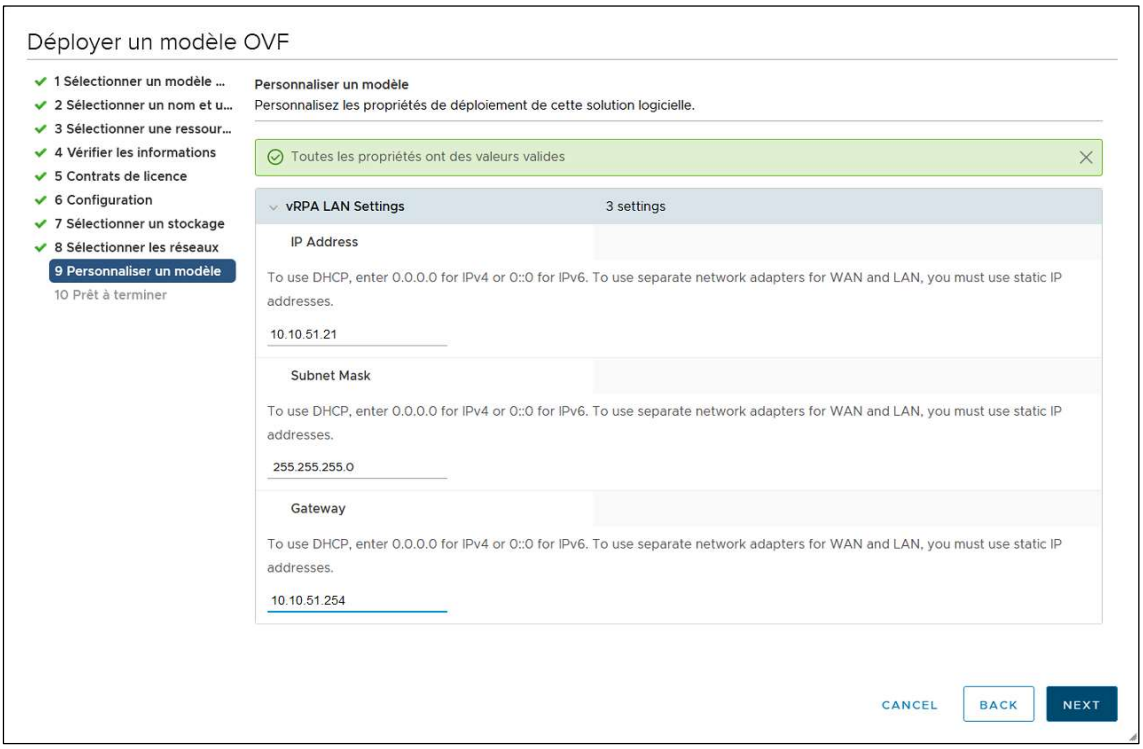


Figure 21 - Configuration IP de l'appliance vRPA

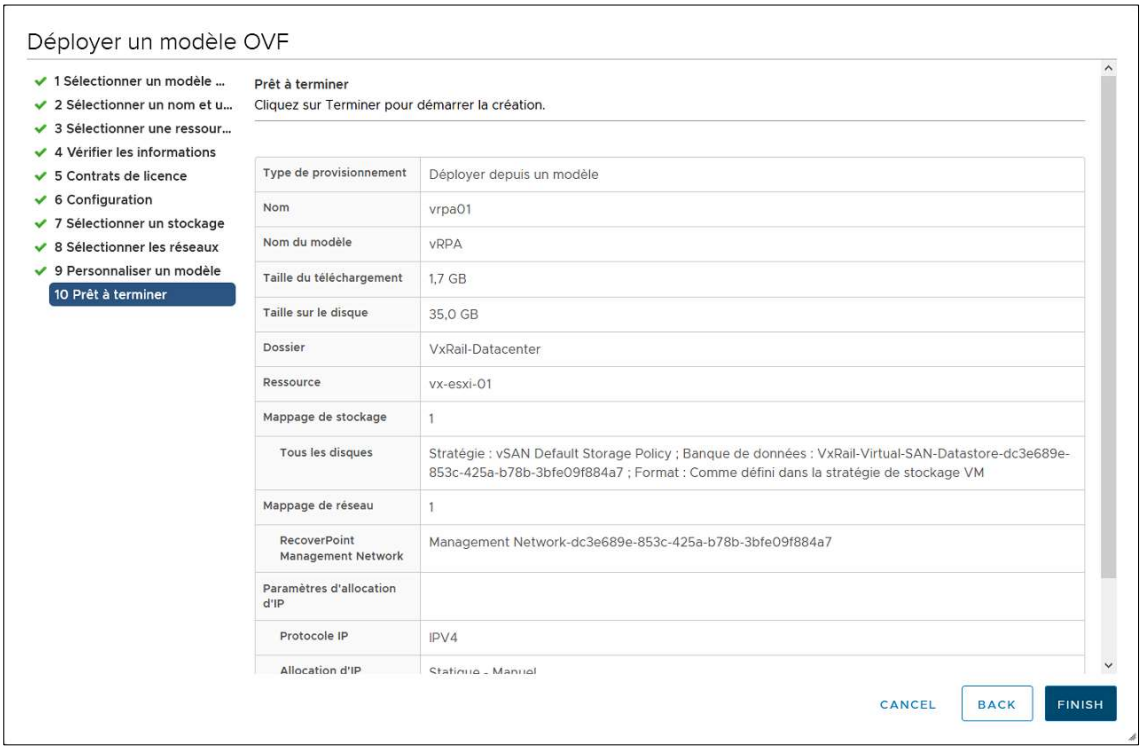


Figure 22 - Validation de la configuration de vRPA

Le déploiement de la première vRPA est terminé, la même opération est utilisée pour déployer la 2ième vRPA du site de Bejaia, ainsi que les deux vRPA du site de Setif.

3.4. Déploiement du Plugin Server

Plugin Server peut être aussi téléchargé comme un modèle OVF et installé de la même façon que les appliances vRPA.

3.5. Configuration du Cluster vRPA

Après avoir installé deux appliances vRPA et un Plugin Server dans chaque site, nous allons maintenant créer un Cluster vRPA dans chaque site, les deux clusters seront connectés entre eux plus tard :

Pour créer un cluster vRPA, nous allons nous connecter à l'une des appliances vRPA déjà déployées en utilisant son adresse IP dans un navigateur web, les étapes de création du cluster sont illustrées dans les figures de 23 jusqu'à 29 :

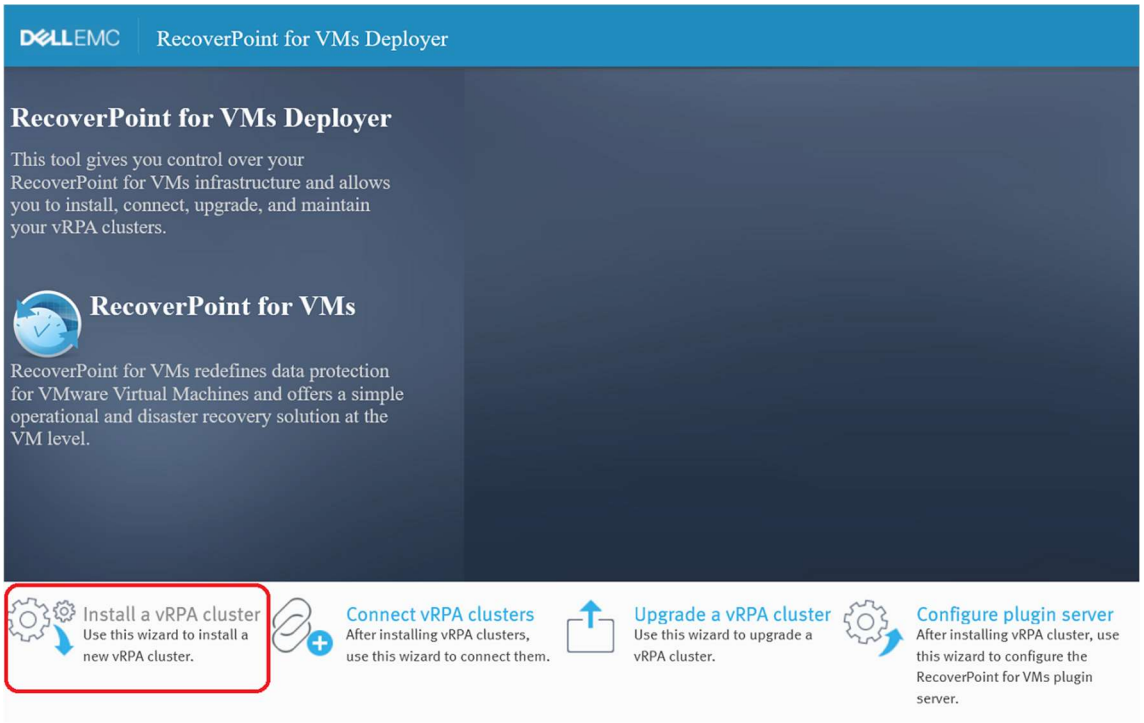


Figure 23 - Création d'un cluster vRPA à partir d'une appliance.

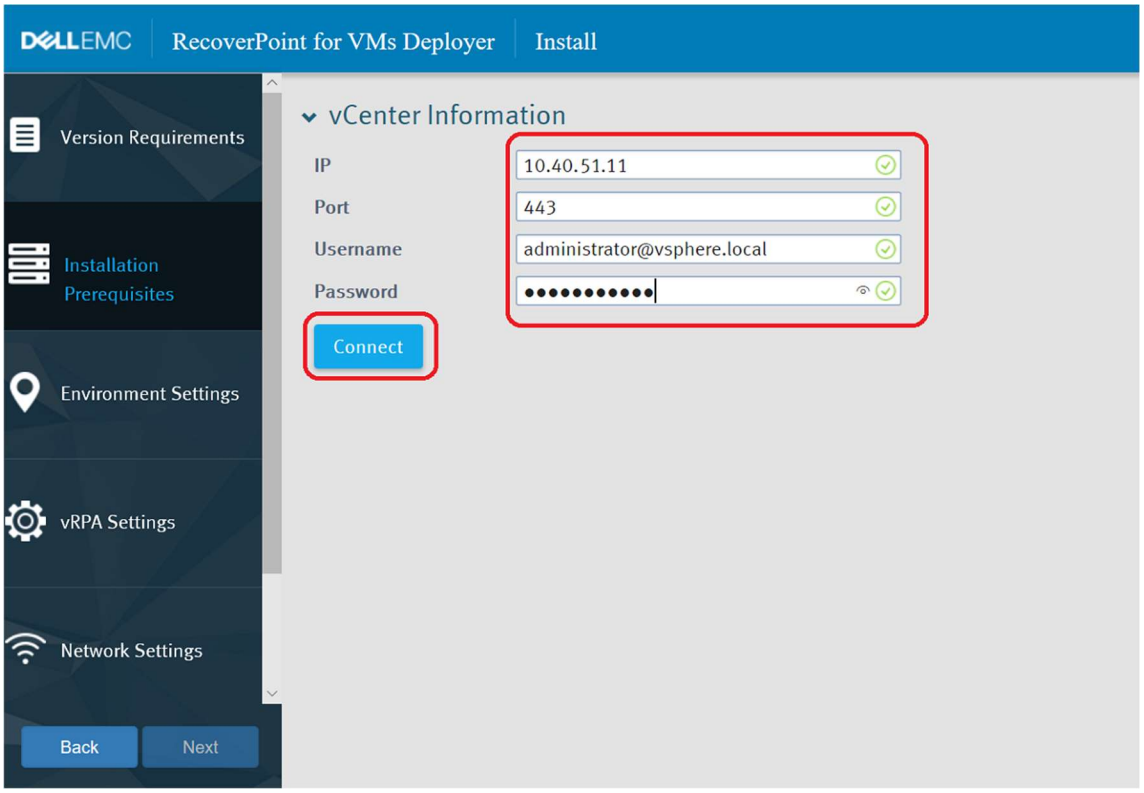


Figure 24 - Authentification dans vCenter.

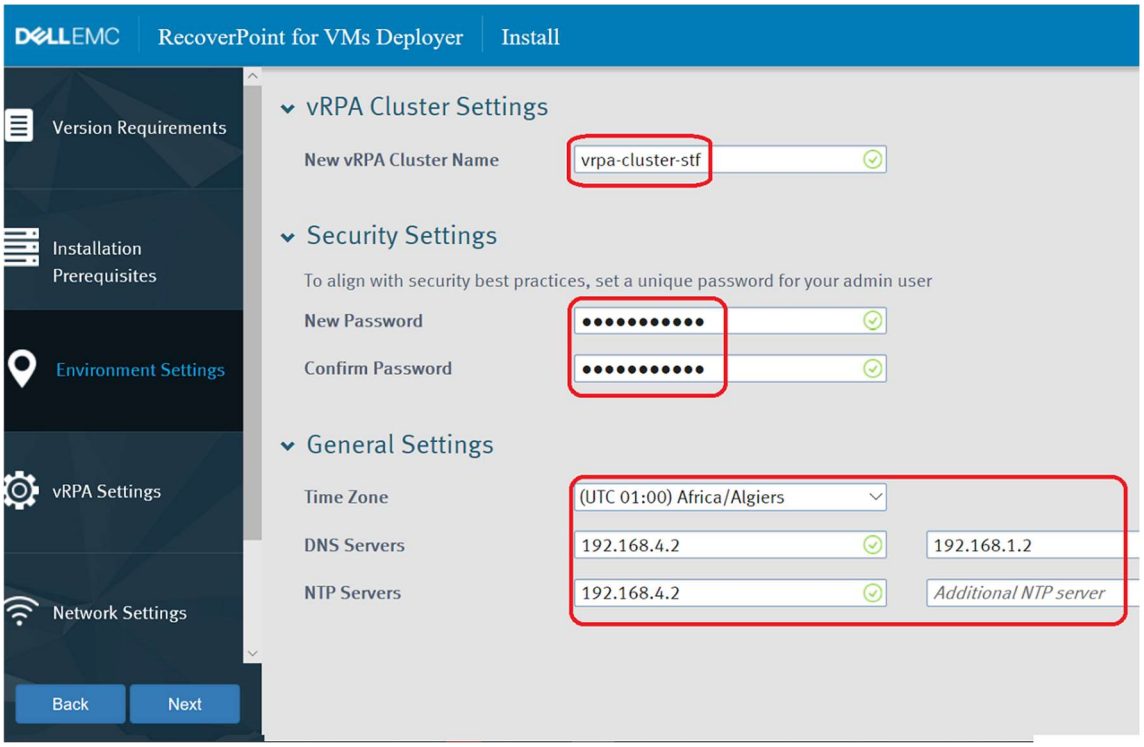


Figure 25 - Configuration de l'environnement du cluster.

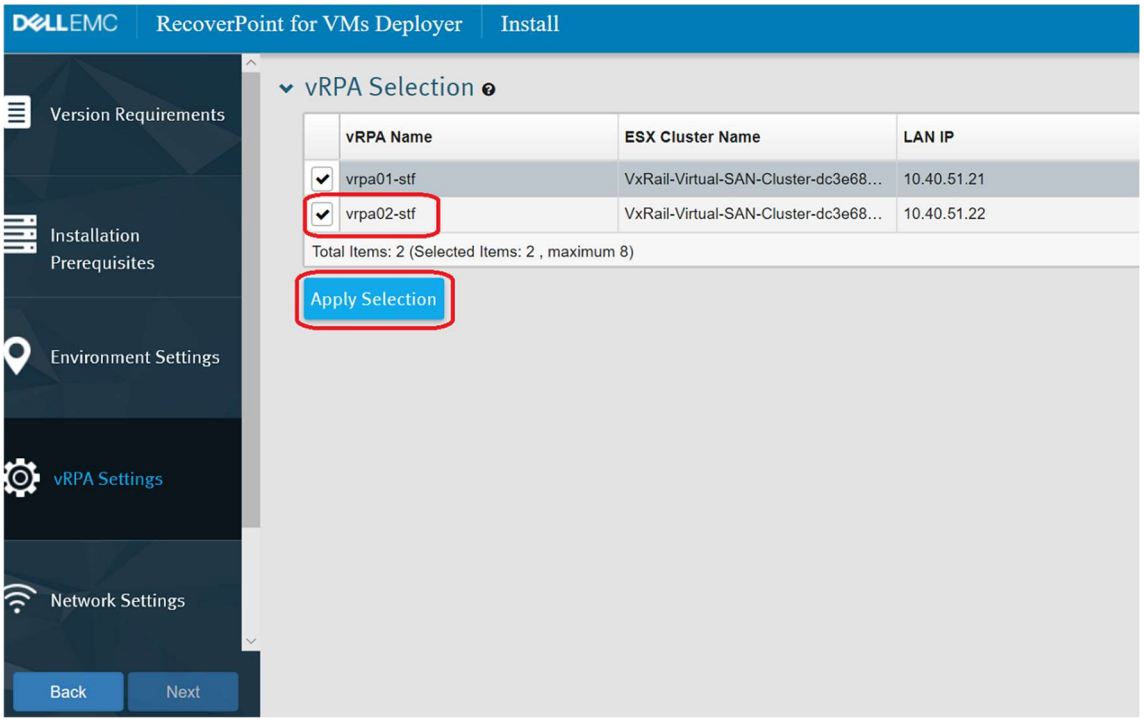


Figure 26 - Ajouts des appliances vRPA au cluster.

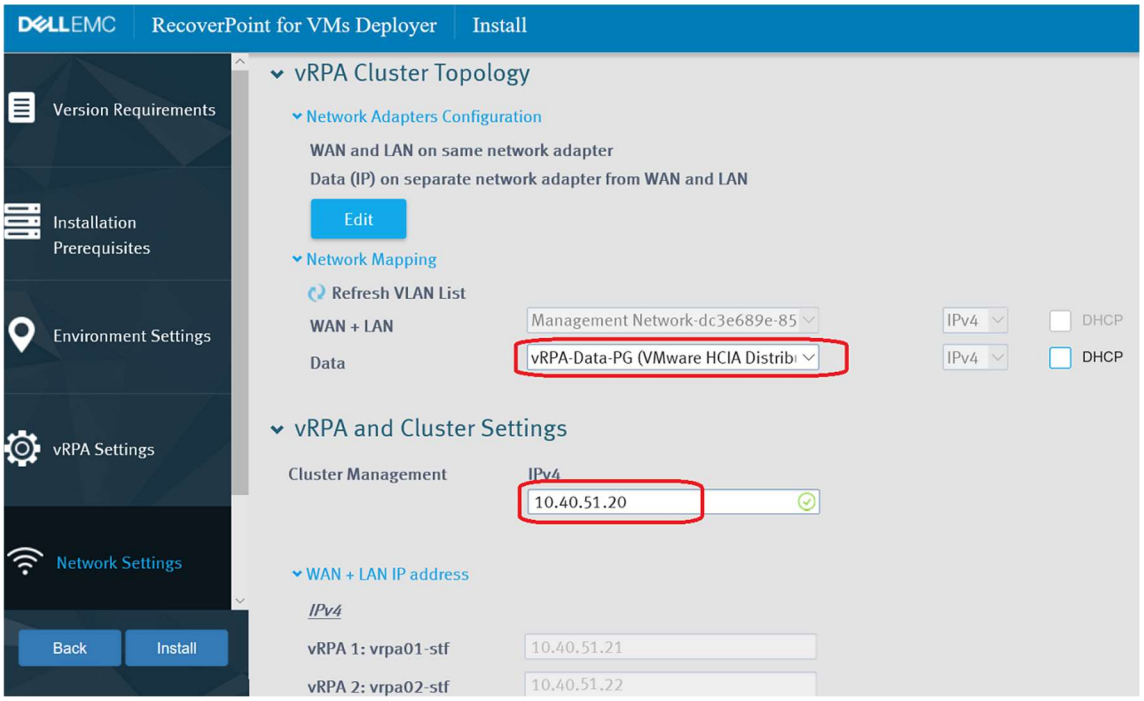


Figure 27 - Configuration réseau du cluster.

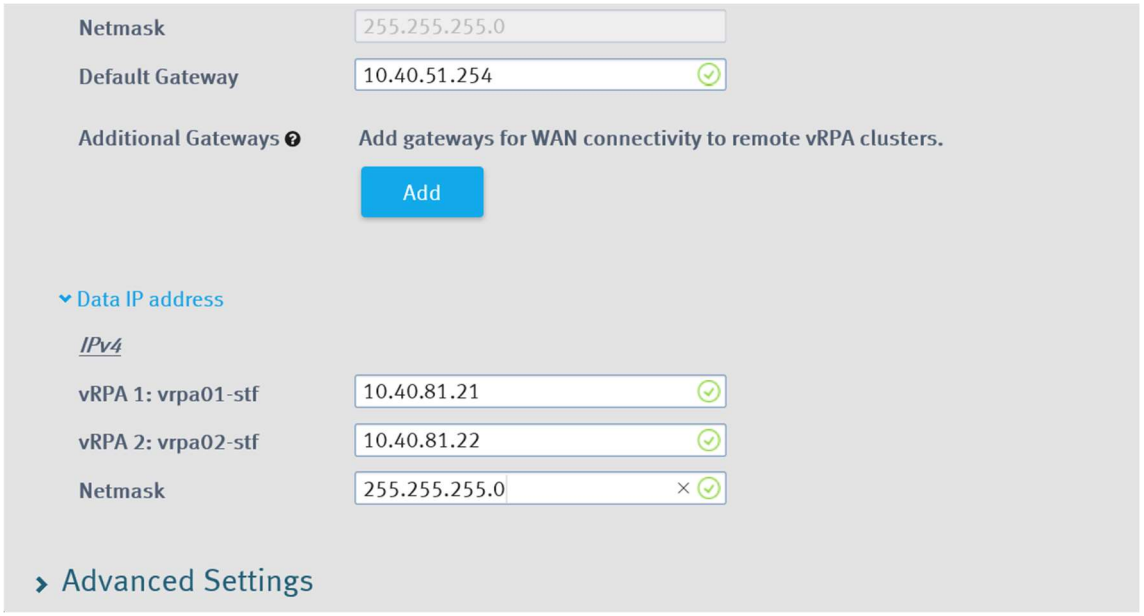


Figure 28 - Configuration réseau du cluster - suite.

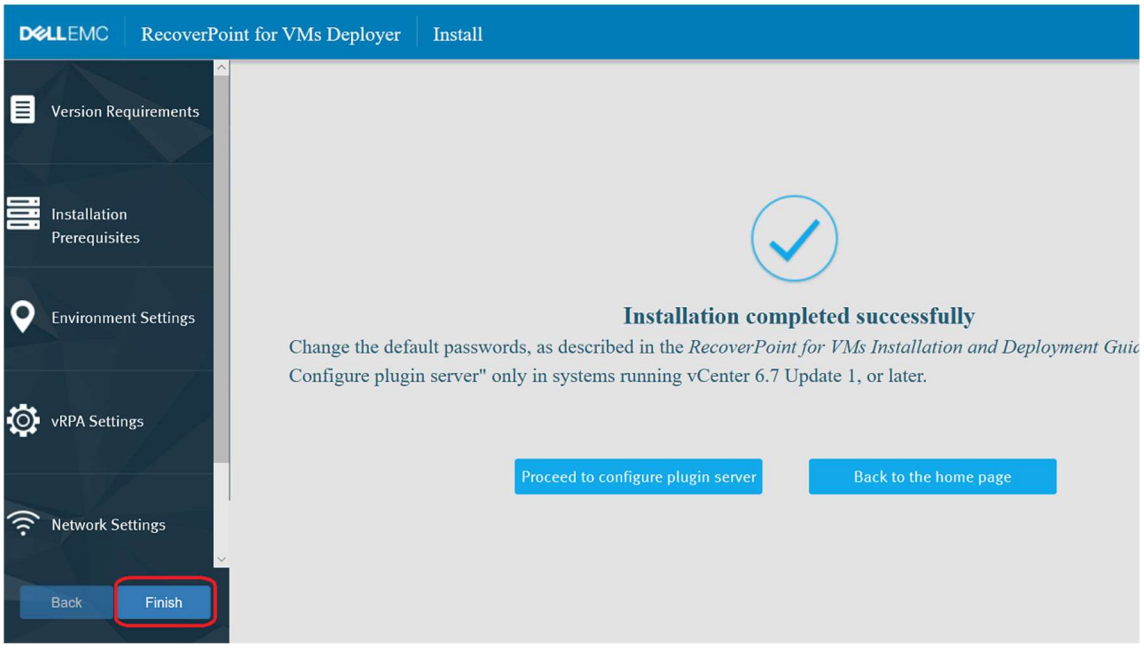


Figure 29 - Validation de la configuration.

Nous avons configuré un cluster sur un site, il faut refaire les mêmes étapes sur l'autre site pour créer un autre cluster.

Une fois les deux clusters sont configurés, il faut procéder à la configuration du vRPA System Cluster entre les deux sites, pour le faire il suffit de se connecter à l'une des 4 appliances vRPA ou l'un des deux clusters (en utilisant son adresse IP dans un navigateur web) et suivre le wizard.

Les étapes de configuration sont illustrées dans les figures 30, 31 et 32 :

Figure 30 - Connexion des deux clusters vRPA.

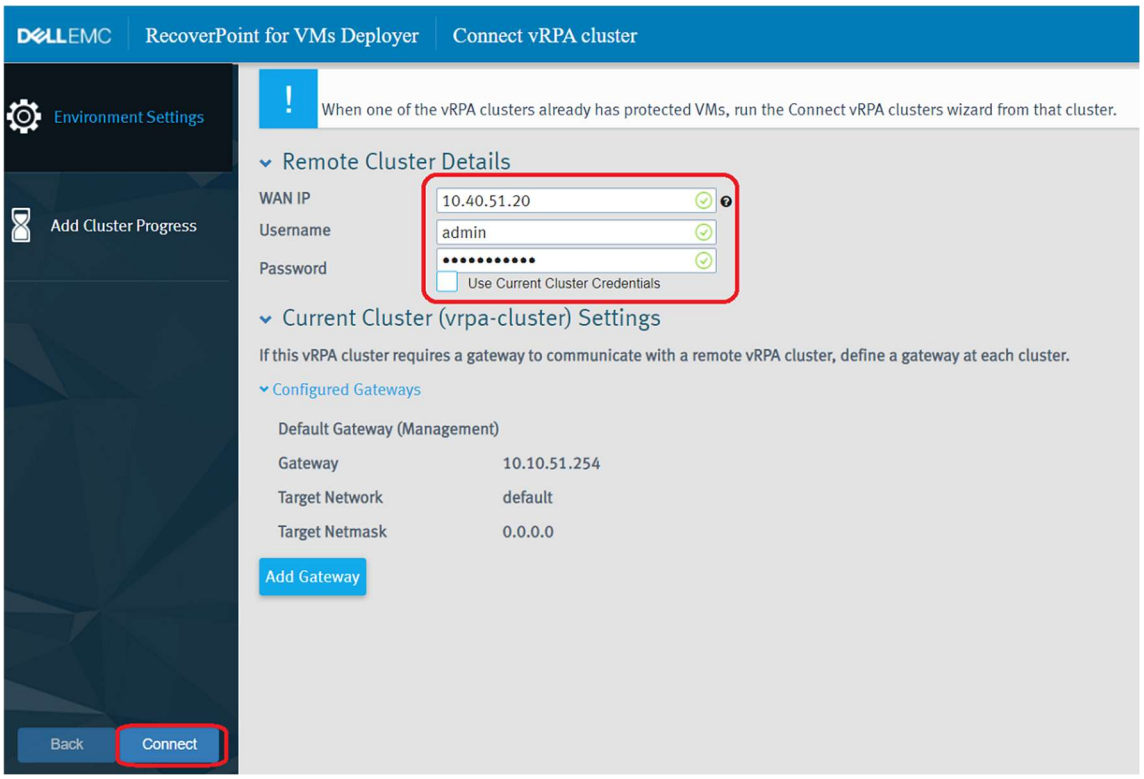


Figure 31 - Définition de l'adresse IP du cluster distant.

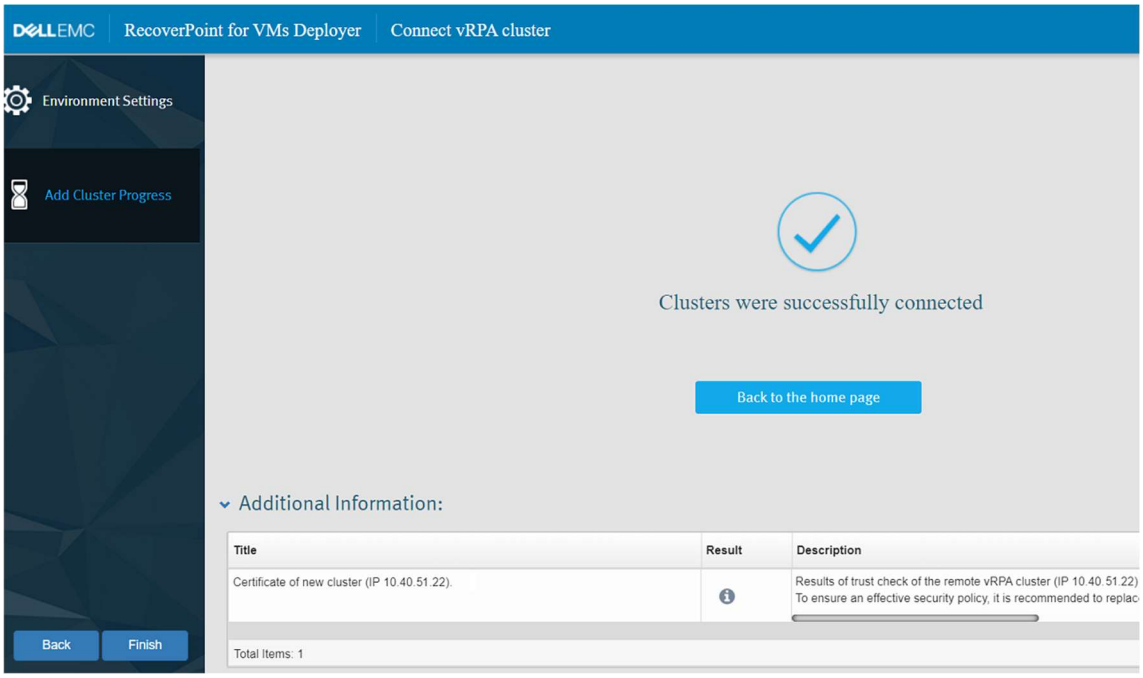


Figure 32 - Les deux clusters sont désormais connectés.

Une fois la configuration est terminée, nous pourrons voir le RecoverPoint dans vCenter (voir la figure 33).

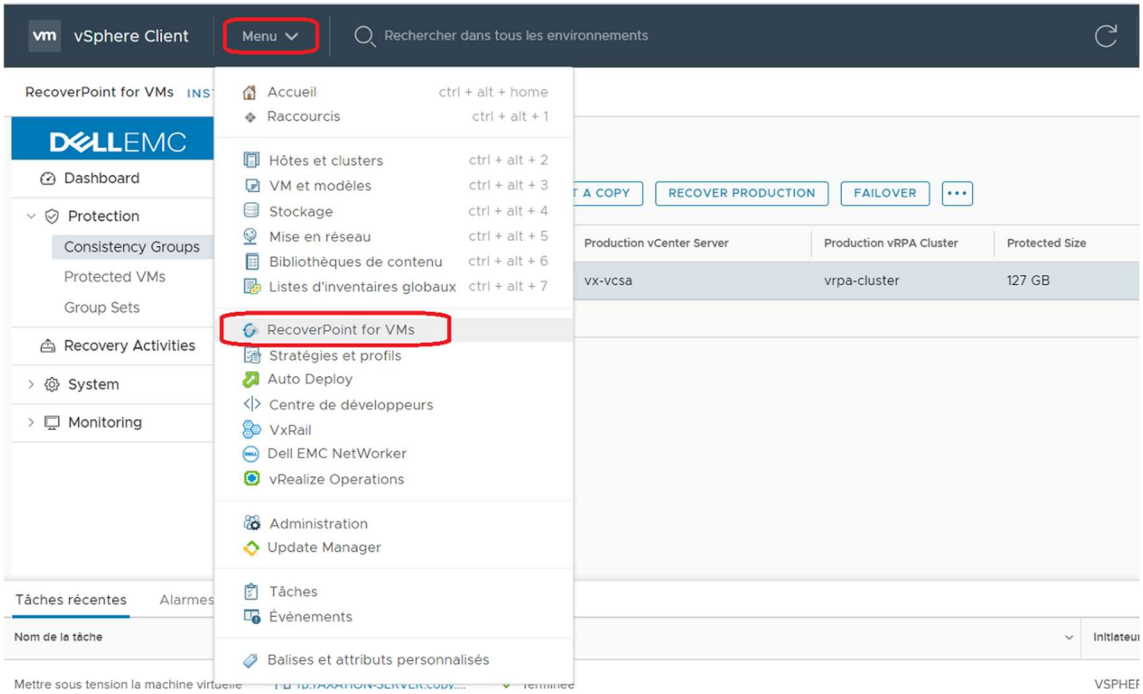


Figure 33 - RecoverPoint for VMs est accessible à partir du vCenter.

4. Protection d'une VM

A partir du poste de travail DSI-03 (voir figure 34), on peut voir que le serveur na-server est accessible et il a bien l'adresse IP 192.168.1.70 (voir les figures 35 et 36).

L'utilisateur arrive à pinger le serveur, et accéder à ce dernier avec une connexion Bureau à Distance (voir la figure 37).

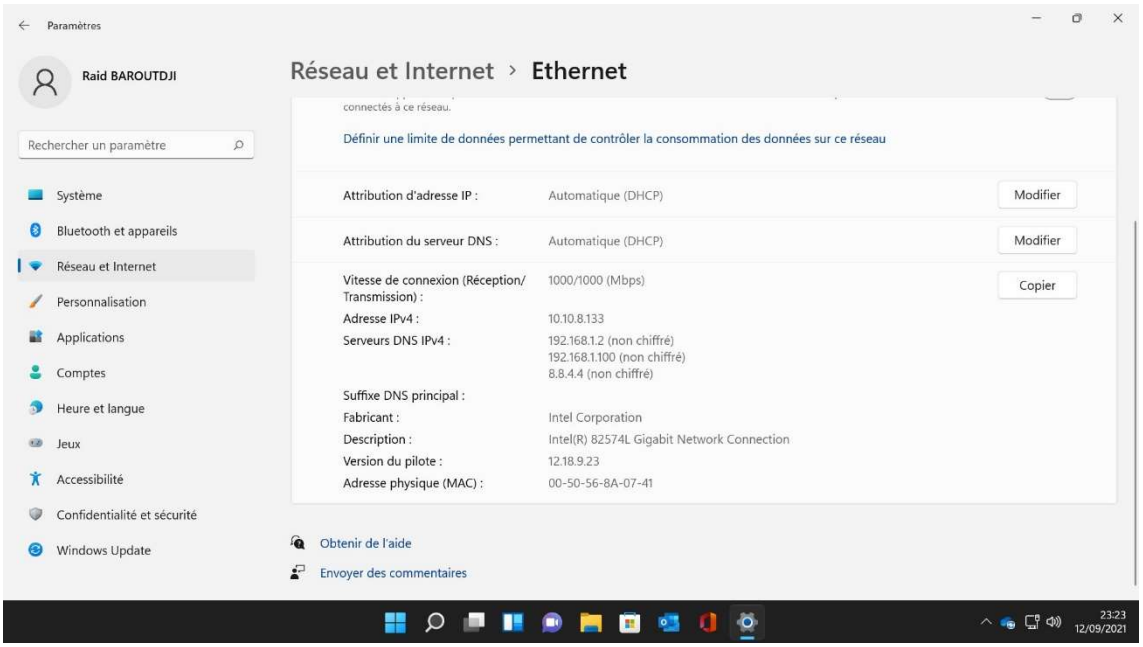


Figure 34 - Propriétés de poste de travail DSI-O3

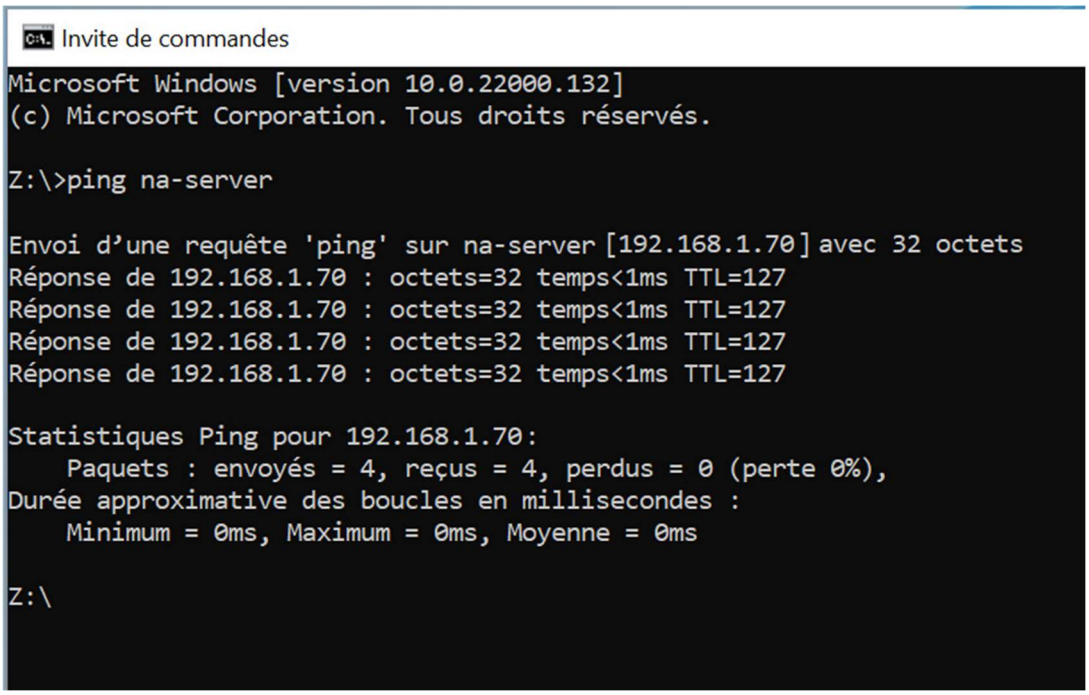


Figure 35 - Test de ping du serveur na-server à partir du poste client.

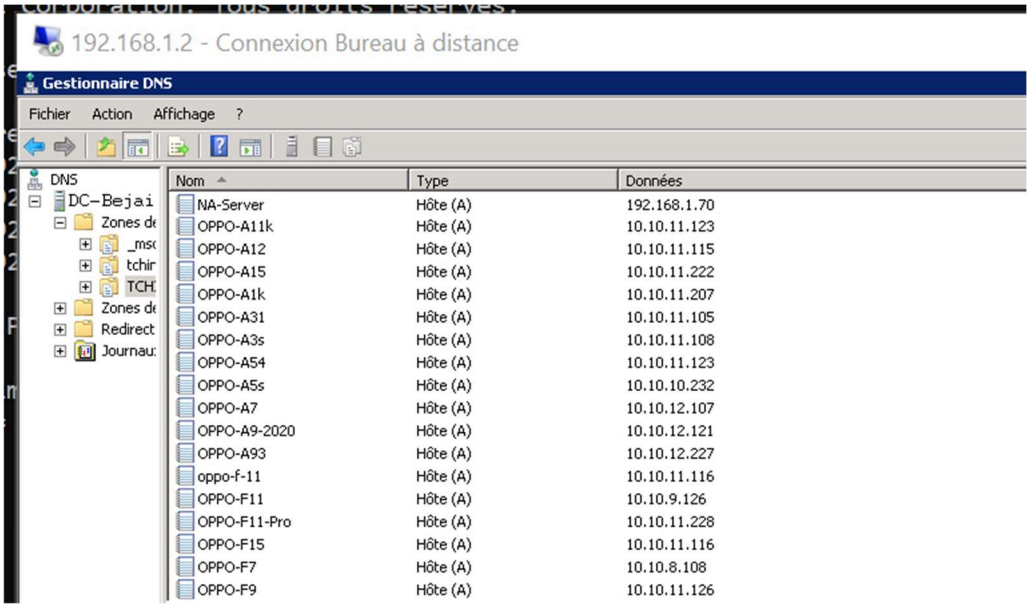


Figure 36 - Enregistrement DNS du serveur na-server

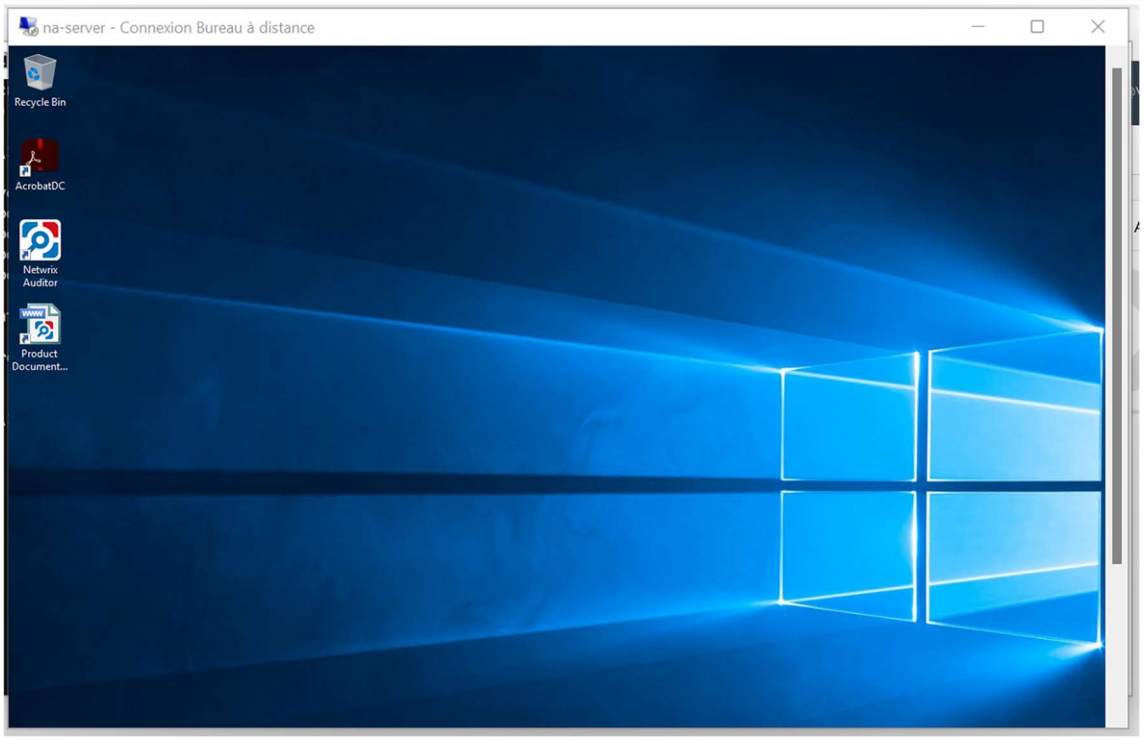


Figure 37 - Connexion en RDP au serveur na-server à partir du poste client.

Maintenant nous allons procéder à la protection du serveur na-server à l'aide de RecoverPoint, en le dupliquant sur le site de secours.

A partir de l'interface web du vCenter, on peut protéger la VM en cliquant sur « Protect VM … » dans le menu contextuel (voir la figure 38).

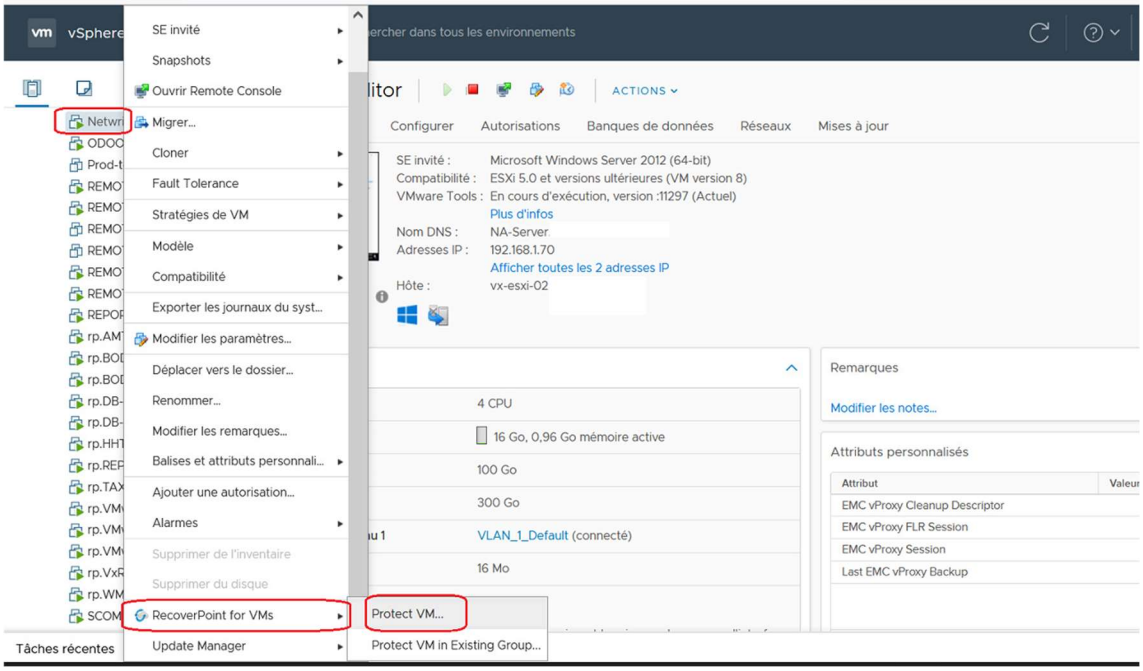


Figure 38 - Protection de la VM à l'aide de RecoverPoint.

Dans la fenêtre qui apparait (figure 39), l'utilitaire propose automatiquement de créer une copie distante (sur le cluster distant qu'on vient de créer), on peut aussi ajouter une autre copie locale en cliquant sur « +ADD A COPY ».

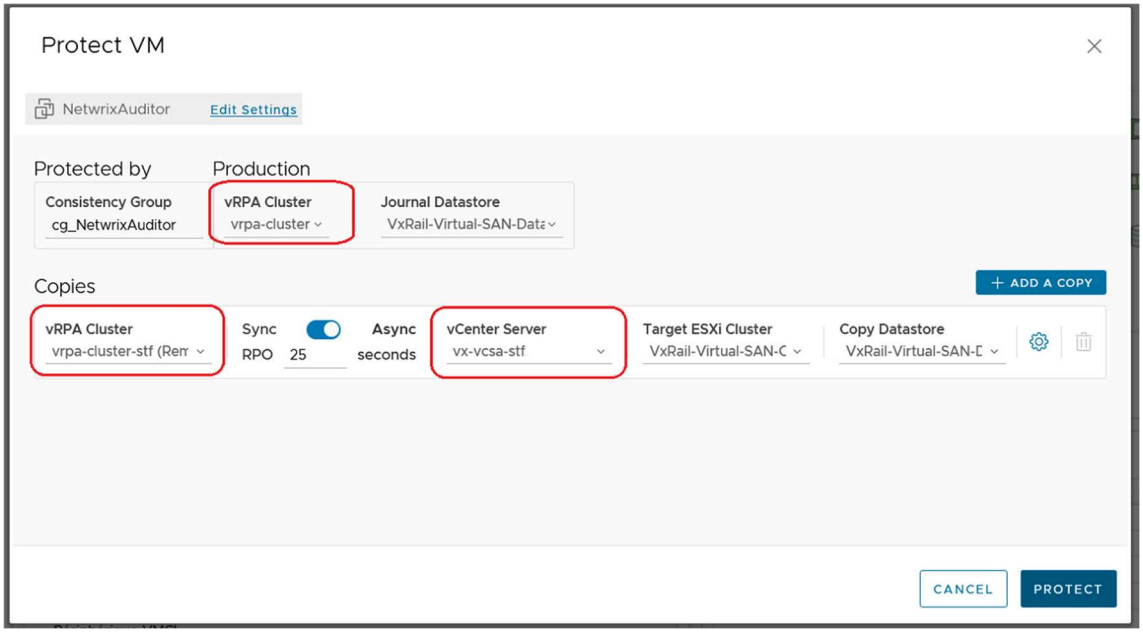


Figure 39 - Création d'une copie distante.

Une fois la copie est créée, nous allons accéder au Plugin Server pour configurer cette copie de VM, comme montré dans les figures 40 et 41.

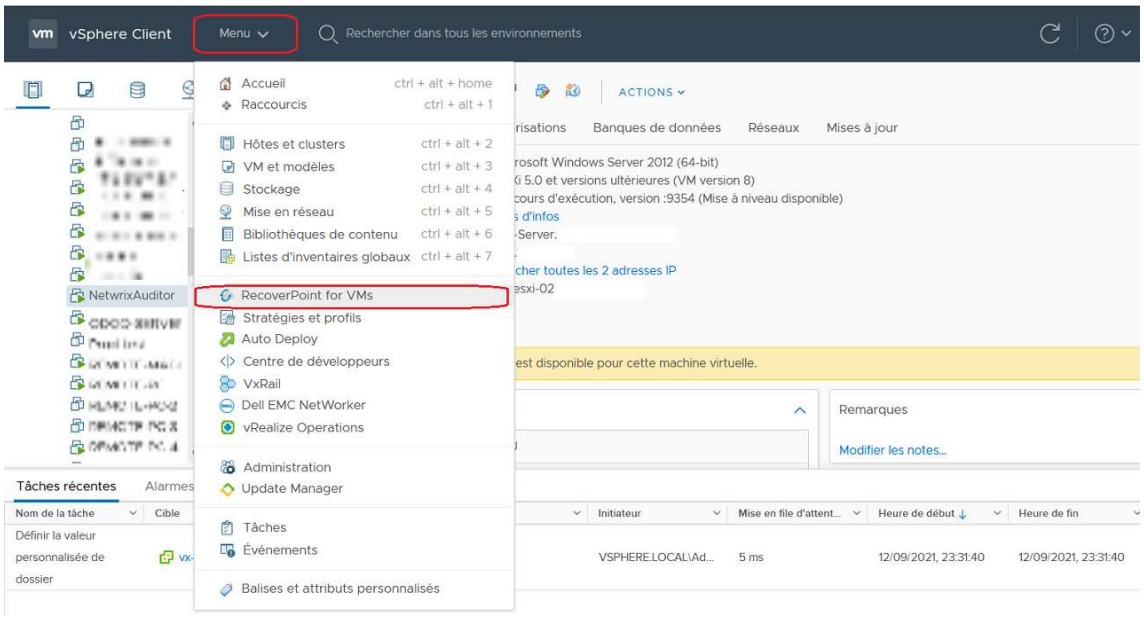


Figure 40 - Accès à RecoverPoint à partir de vCenter.

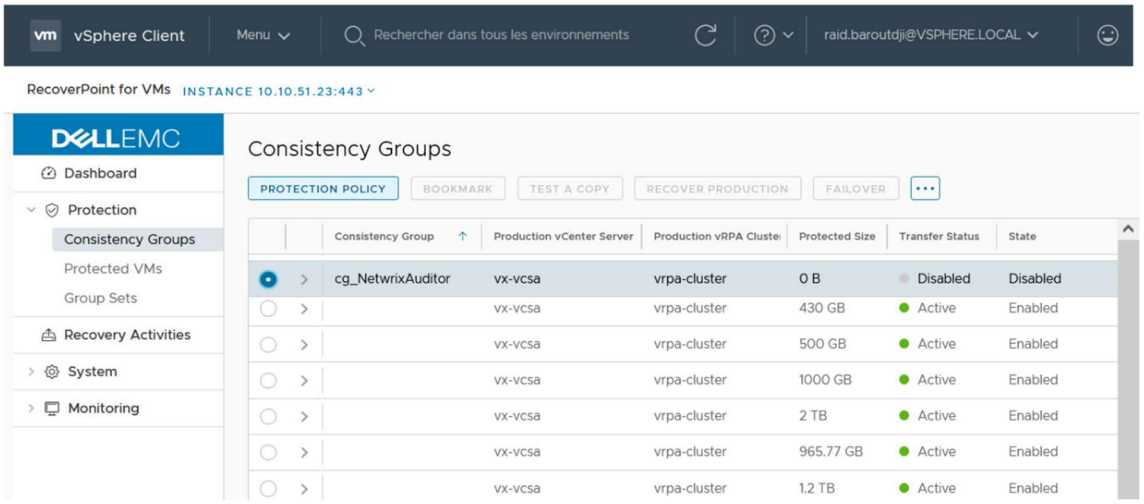


Figure 41 - La copie est créée.

Maintenant il faut faire certaines personnalisations, à savoir le nom DNS et la configuration réseau que la VM va avoir sur le site de secours (voir les figures 42 et 43).

Pour que ça soit transparent à l'utilisateur final, nous allons garder le même nom DNS, et configurer une nouvelle adresse IP valable au niveau du site distant, et nous comptons sur les serveurs DNS pour faire correspondre ce nom à la nouvelle adresse IP que la VM.

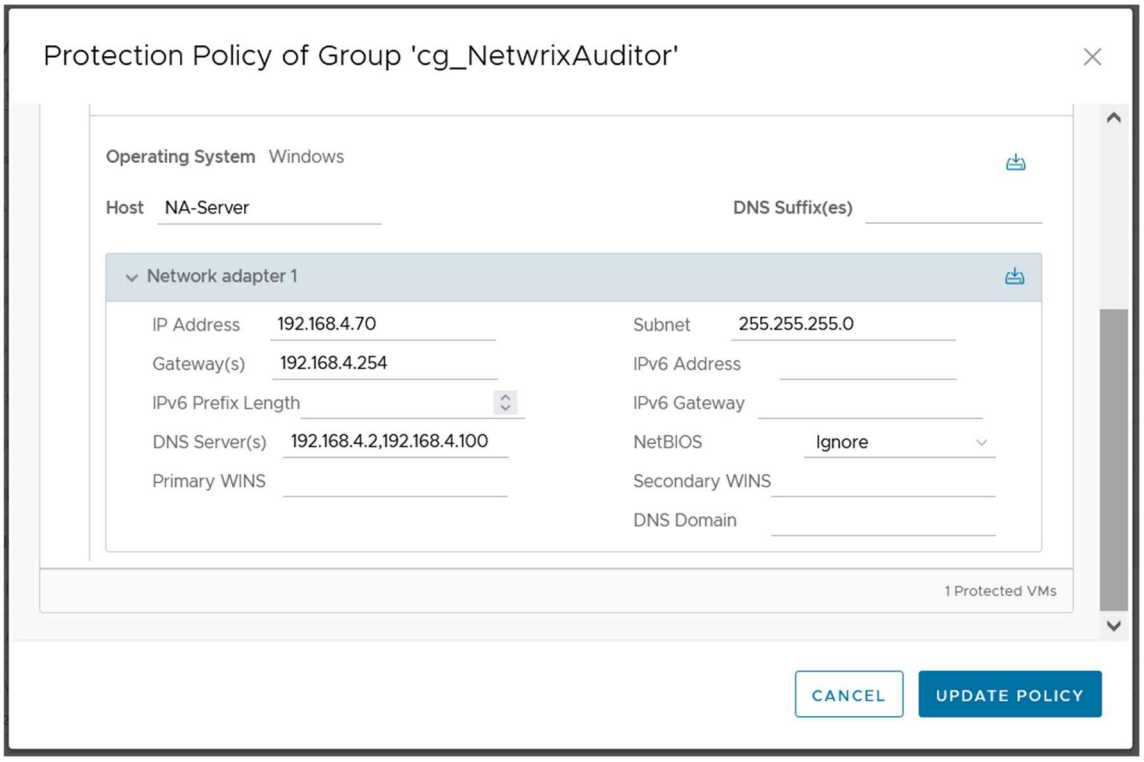


Figure 42 - Configuration de l'IP distante de la VM.

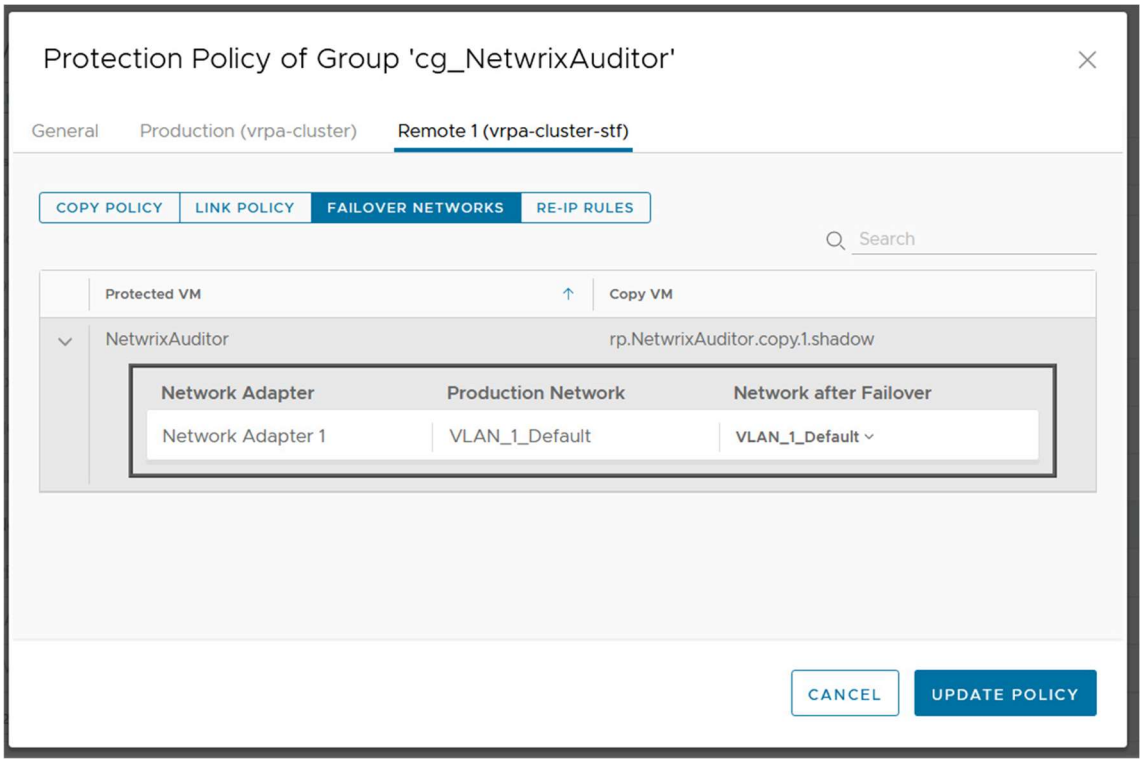


Figure 43 - Définir le réseau distant sur lequel la VM sera connectée.

Une fois la configuration terminée, il faut attendre la synchronisation de la VM avec la nouvelle copie distante, cela peut prendre beaucoup de temps et ça dépend du débit disponible entre les deux sites.

Une fois la configuration terminée, il faut attendre la synchronisation de la VM avec la nouvelle copie distante, cela peut prendre beaucoup de temps et ça dépend du débit disponible entre les deux sites (voir les figures 44 et 45).

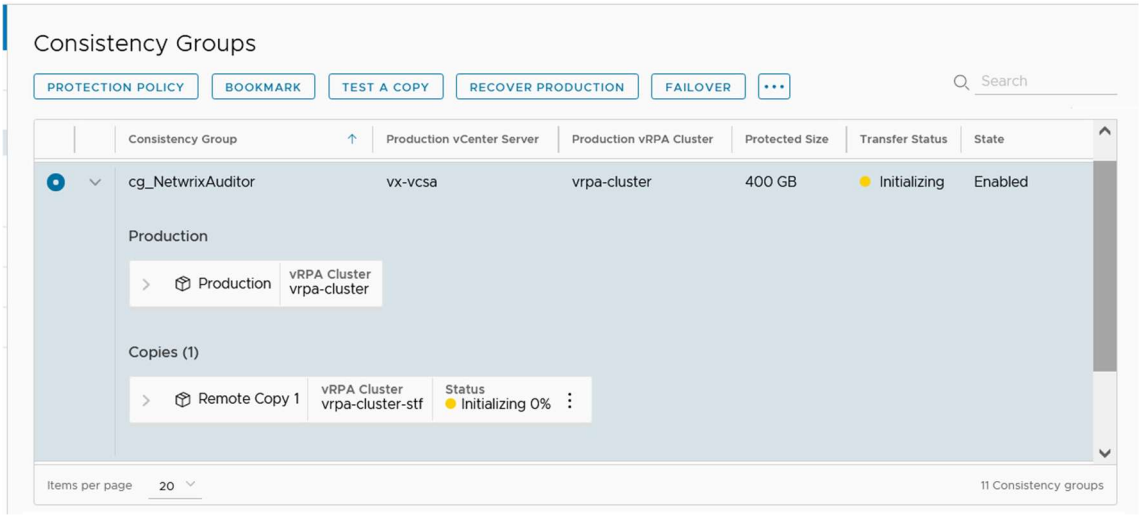


Figure 44 - Initialisation de la copie.

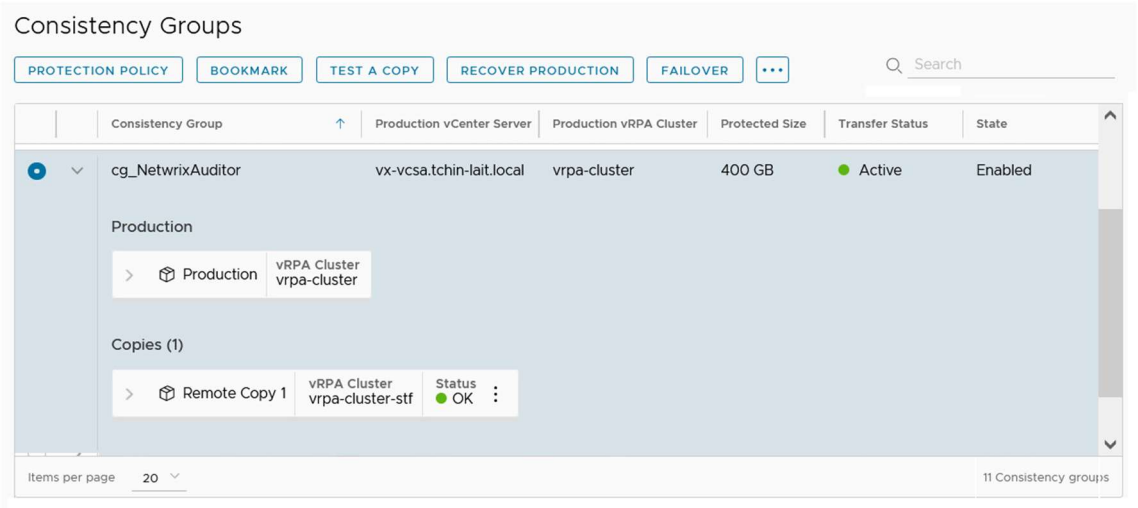


Figure 45 - La copie est prête sur le cluster distant.

5. Test de basculement

En cas d'un désastre, le basculement doit se faire à partir du site distant (comme illustré dans la figure 46), car le site principal est inaccessible, sinon, dans le cas ou seulement la VM est endommagée ou si nous voudrions faire un test, on peut faire le basculement à partir de l'un des deux cluster (local ou distant).

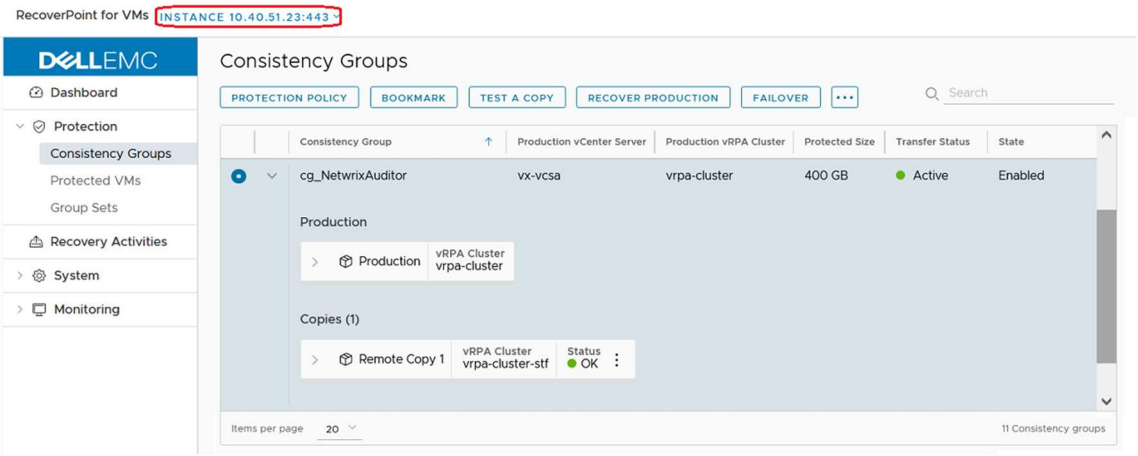


Figure 46 - Accès à RecoverPoint à partir du cluster distant

Avant de lancer une copie d'un VM pour prendre le relai et remplacer la VM originale, nous pouvons procéder au test de cette copie (voir le figure 47), cette étape permet de vérifier l'intégrité et la cohérence de la copie avant de la lancer.

Figure 47 - Test d'une copie de VM.

Au moment de test d'une copie distante (ou locale) le système va démarrer cette dernière, lui attribuer l'adresse IP déjà définie, et le nom DNS défini, mais sans la connecter au réseau de production (pour éviter les conflits), et cela tout en gardant la VM originale en marche, pour ne pas interrompre les services (voir la figure 48).

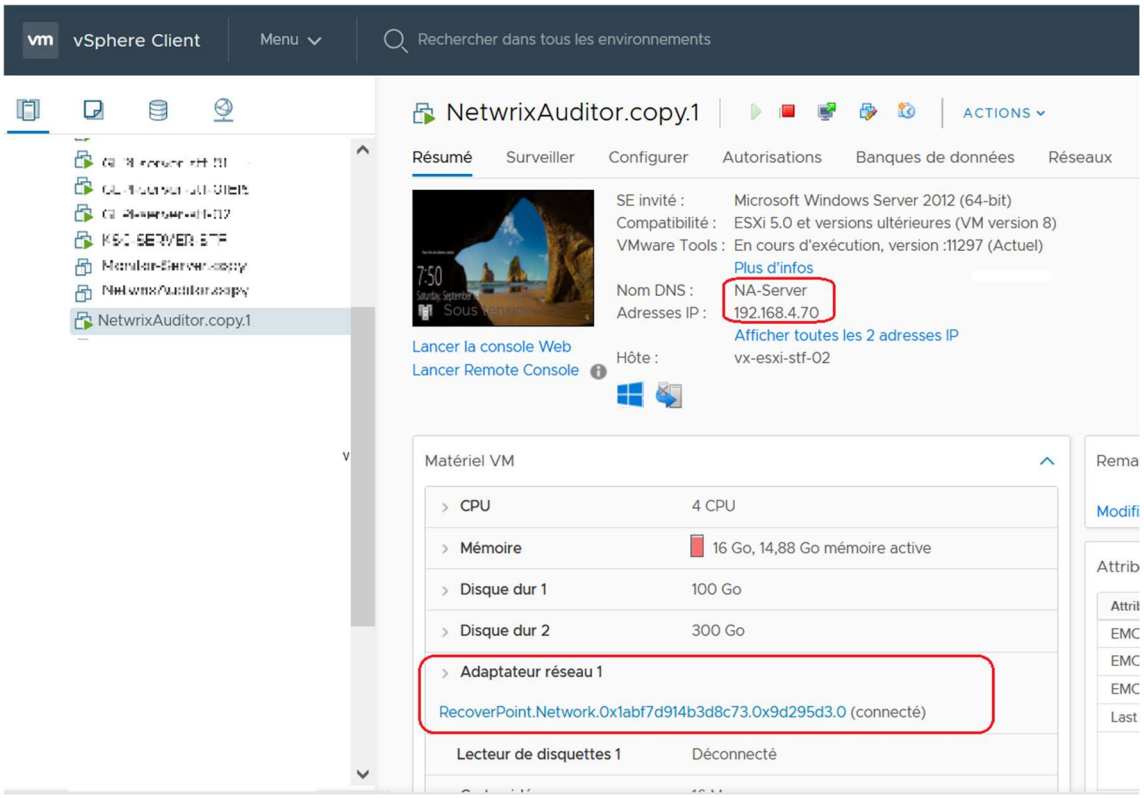


Figure 48 - Démarrage de la copie dans un réseau de test.

Une fois qu'on a vérifié que la copie est intègre et cohérente, nous pourrons lancer le Failover (voir la figure 49), ceci implique le shutdown de la VM de production, la copie qu'on vient de tester est alors connectée au réseau de production avec l'adresse IP et le nom DNS déjà définis comme montré dans la figure 50).

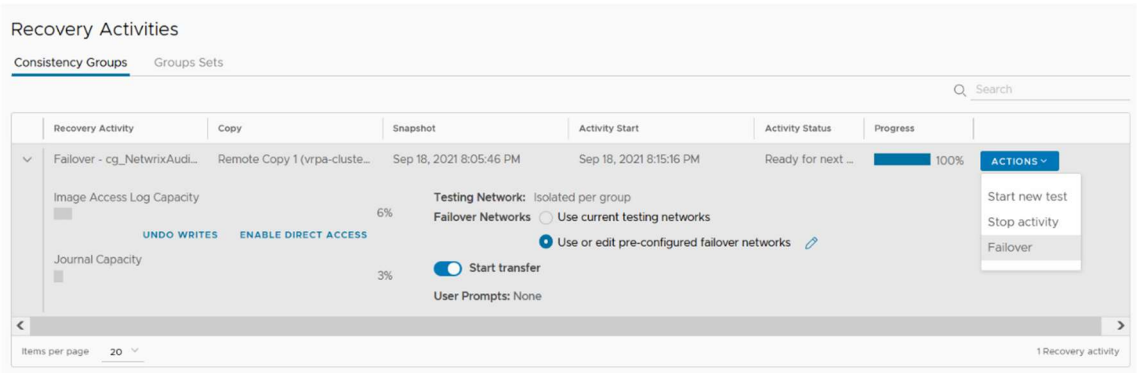


Figure 49 – Lancement d'un Failover sur une copie de VM.

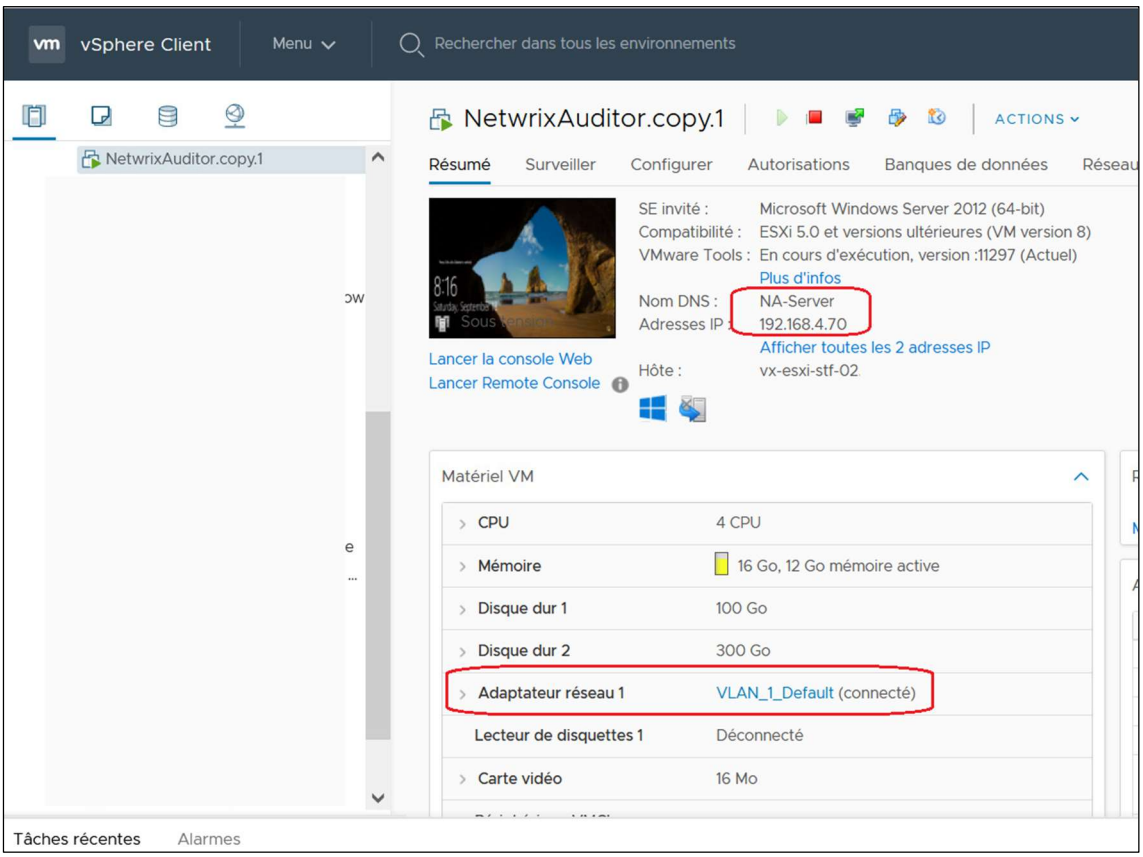


Figure 50 - La VM copie est allumée est connectée au réseau de production.

Après avoir lancé le Failover, il ne nous reste qu'attendre que les serveurs DNS fassent leur travail, c'est à dire, la correction de l'enregistrement DNS (avec la nouvelle adresse IP).

Le serveur DNS qui se trouve sur le site de secours va mettre à jour l'enregistrement DNS immédiatement, mais la synchronisation avec les autres serveurs de l'autre site peut prendre un petit moment, cela dépend de la configuration de la réplication entre les différents serveurs DNS et le débit entre les sites, mais un administrateur peut toujours lancer la synchronisation d'une façon manuelle pour éviter d'attendre.

Entre temps, et en jetant un coup d'œil sur le RecoverPoint, nous remarquons que désormais la réplication se fait dans le sens contraire pour cette VM, c'est-à-dire, qu'après le basculement du serveur **na-server** vers le site de Setif, ce dernier est devenu site principal pour cette VM, donc, automatiquement, la VM est protégée en la répliquant sur le site principal, qui est devenu site de secours pour cette VM (voir la figure 51).

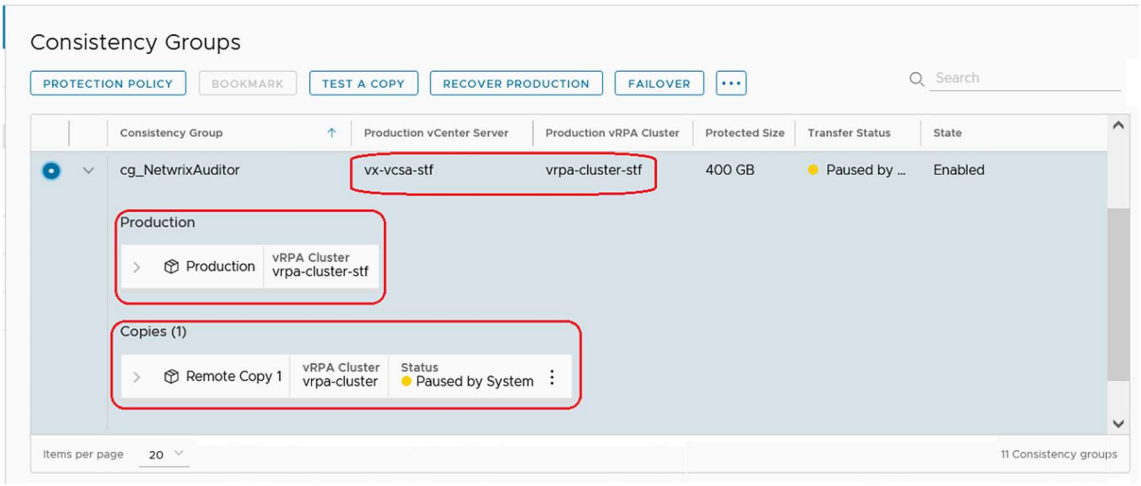


Figure 51 - Réplication de la VM dans le sens inverse.

Dans le cas de notre étude, l'enregistrement DNS a été corrigé et répliqué sur tous les serveur DNS dans un délai de 10 minutes sans intervention humaine (voir la figure 52).

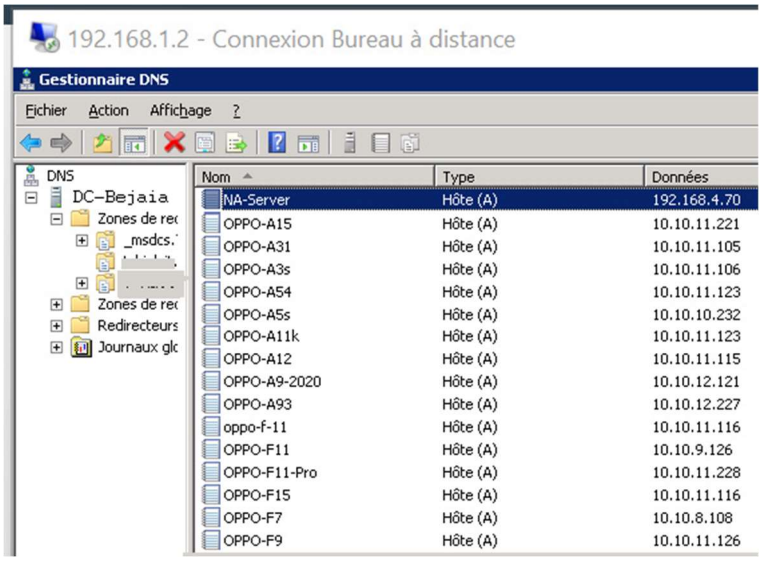


Figure 52 - Enregistrement DNS corrigé sur le serveur DNS.

Le serveur na-server est toujours pingable depuis le poste utilisateur et il renvoie une nouvelle adresse IP (voir la figure 53), et il est toujours accessible en Bureau à Distance en utilisant le même nom DNS comme illustré dans la figure 54.

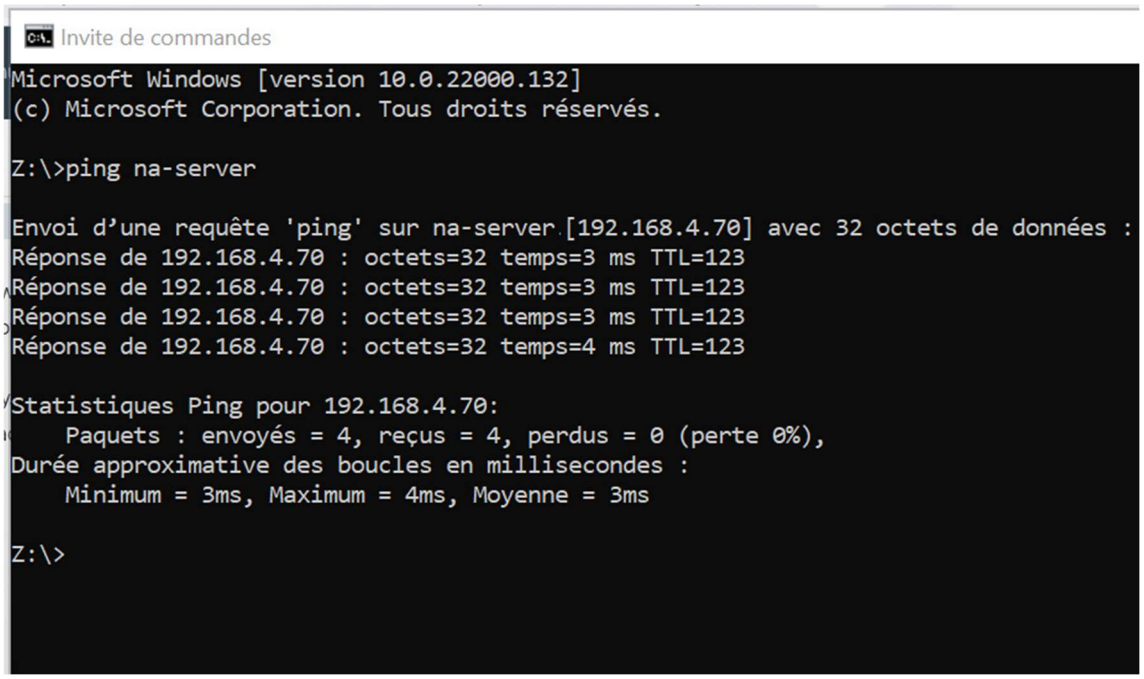


Figure 53 - Test de ping du serveur na-server à partir du poste client.

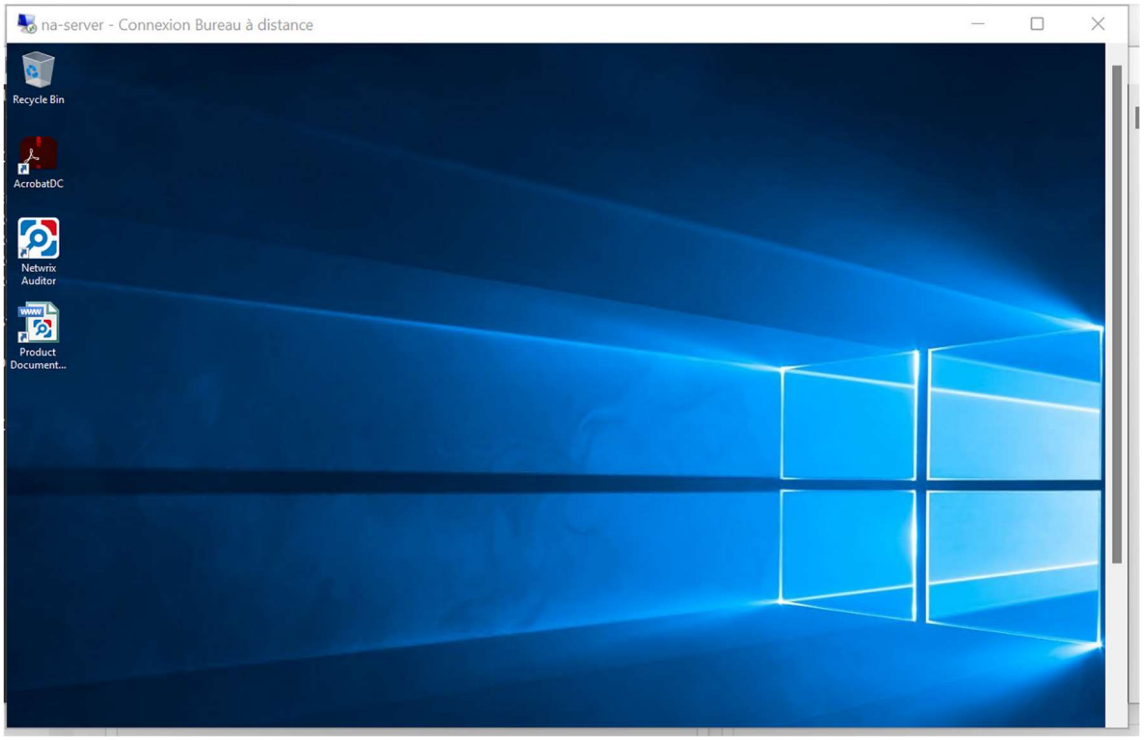


Figure 54 - Connexion en RDP au serveur na-server à partir du poste client.

6. Conclusion

Dans ce chapitre, nous avons vu comment mettre en œuvre la solution proposée à savoir RecoverPoint for Virtual Machines, comment faire la configuration nécessaire pour protéger les données en cas de désastre.

Nous avons vu aussi comment protéger une VM en la dupliquant sur un site distant, et comment reprendre le service sur ce site après l'avoir arrêté sur le site principal, d'une façon transparente par rapport à l'utilisateur final, ce dernier n'a eu aucune procédure à faire pour reprendre le service, on peut dire qu'il n'a même pas senti un changement ou un basculement d'un site à un autre.

Conclusion Générale et Perspectives

Le développement accéléré de l'informatique et des technologies de communication, a transformé le monde en un petit village où tout est connecté.

Actuellement, chaque individu manipule, stocke et partage des données. La quantité des informations stockées et partagées dans le monde n'a jamais été aussi importante auparavant.

Au moment où beaucoup d'entreprises optent pour stocker leurs données en cloud, d'autres préfèrent de les gérer eux-mêmes dans leurs propres data centers implantés dans différents endroits dans le monde entier. Le choix de l'endroit dépend de plusieurs facteurs, comme la sécurité et la stabilité de l'alimentation électrique et des liaisons de communication.

Beaucoup d'organismes accèdent à leurs données à partir de plusieurs endroits différents reliés au data center par des liaisons sécurisées, comme le cas des séries de boutiques ou d'hypermarchés. La protection de ces données contre les attaques et les pertes est un point essentiel pour assurer la continuité du service.

Dans ce mémoire de master avons proposé et mis en place une solution de reprise d'activité après un sinistre (Disaster Recovery Solution), qui permet de protéger les données sensibles en dupliquant des machines virtuelles complètes sur un site distant.

Plusieurs solutions peuvent être proposées pour protéger les données, comme la sauvegarde par exemple. Cependant, les solutions de sauvegarde prennent, dans certains cas, beaucoup de temps pour rétablir la situation, d'où, une solution de reprise de service en temps réel s'impose.

La solution que nous avons proposée permet à une copie de VM stockée sur un site distant, et synchronisée en temps réel, de prendre le relai en cas d'arrêt de la VM de production sur le site principal.

L'intérêt d'une telle solution est la possibilité de reprendre l'activité après une catastrophe naturelle, par exemple, soit à partir d'une copie locale ou à distance, dans notre cas, nous nous sommes intéressés à la duplication à distance.

Dans la continuité de nos travaux de mémoire de Master, nous proposons les perspectives suivantes :

- Mettre en œuvre une solution de sauvegarde pour épauler RecoverPoint, en sauvegardant les autres VMs qui ne nécessitent pas une reprise de

service en temps réel, sur une baie de stockage, ces mêmes sauvegardes peuvent être dupliquées sur le site distant pour éviter toute perte.

- Tester la solution RecoverPoint sur d'autre plateformes autres que VMware (Hyper-V par exemple).
- Améliorer le lien entre les deux sites, en dupliquant les liaisons VPN, de façon d'avoir deux liaisons VPN, avec deux partenaires différents, et un mécanisme de basculement automatique d'une liaison à une autre en cas de coupure.

Annexe A : Netwrix Auditor

Netwrix Auditor (voir figures 55 et 56) est un logiciel d'audit informatique, Netwrix peut alléger le fardeau des audits internes et externe et atteindre des objectifs en déployant beaucoup moins d'efforts. Ses capacités de renseignement prêtes à l'emploi permettent d'automatiser un grand nombre de tâches liées à la sécurité, à la conformité et aux opérations informatiques qui nécessitaient auparavant des heures de travail. [4]

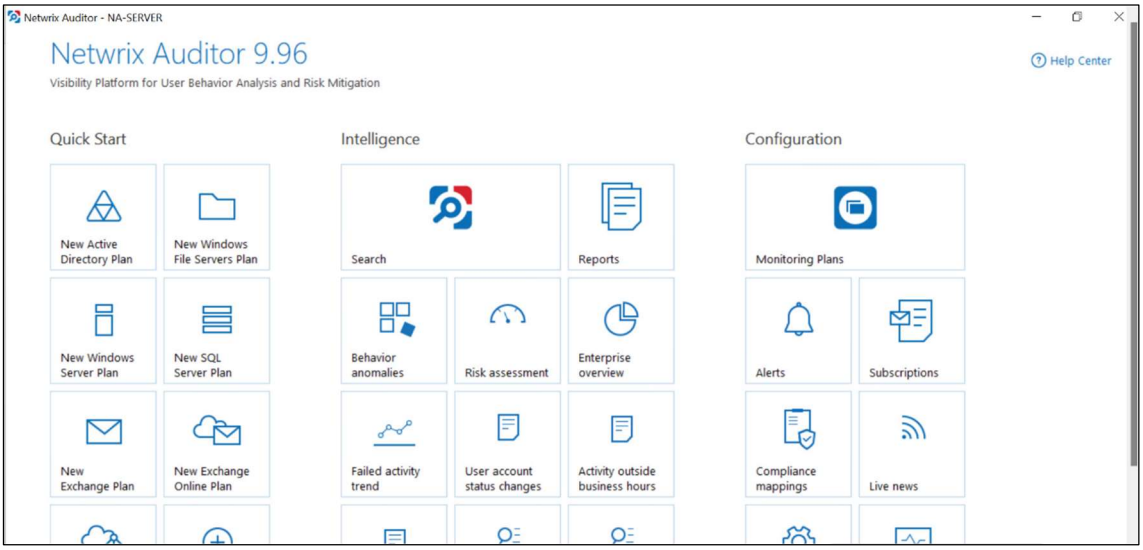


Figure 55 - Netwrix Auditor

Risk Assessment Overview

Risk name	Current value	Risk level
Users and Computers		
User with Password never expires	2	Medium (1-4)
User with Password not required	0	Low (0)
Inactive user accounts	10% (3 of 30)	High (1% - 100%)
Inactive computer accounts	20% (4 of 20)	High (3% - 100%)
Permissions		
User accounts with administrative permissions	20% (6 of 30)	High (3% - 100%)
Empty security groups	6% (0 of 50)	Low (0)
Data		
Shared folders accessible by Everyone	11% (1685 of 15321)	Medium (5% - 15%)
File names containing sensitive data	2	High (2 - unlimited)
Potentially harmful files on file shares	0	Low (0)
Direct permissions on files and folders	21% (10759 of 51237)	High (5% - 100%)

Figure 56 - Risk Assessment - Netwrix Auditor

Annexe B : Centreon Monitoring

Vu que la réplication des machines virtuelles d'un site à un autre dépend du débit disponible au niveau de chaque site, aussi cette opération consomme vraiment de la bande passante au moment de la synchronisation, et pour pouvoir suivre la consommation des ressources, nous avons mis en place une solution de Monitoring Informatique qui supervise l'intégralité des infrastructures IT pour une vue claire et complète. [5]

Cette solution nous permet de contrôler la disponibilité des liaisons VPN, des différents serveurs physiques et virtuels, ainsi que la consommation de la bande passante (voir figure 57).

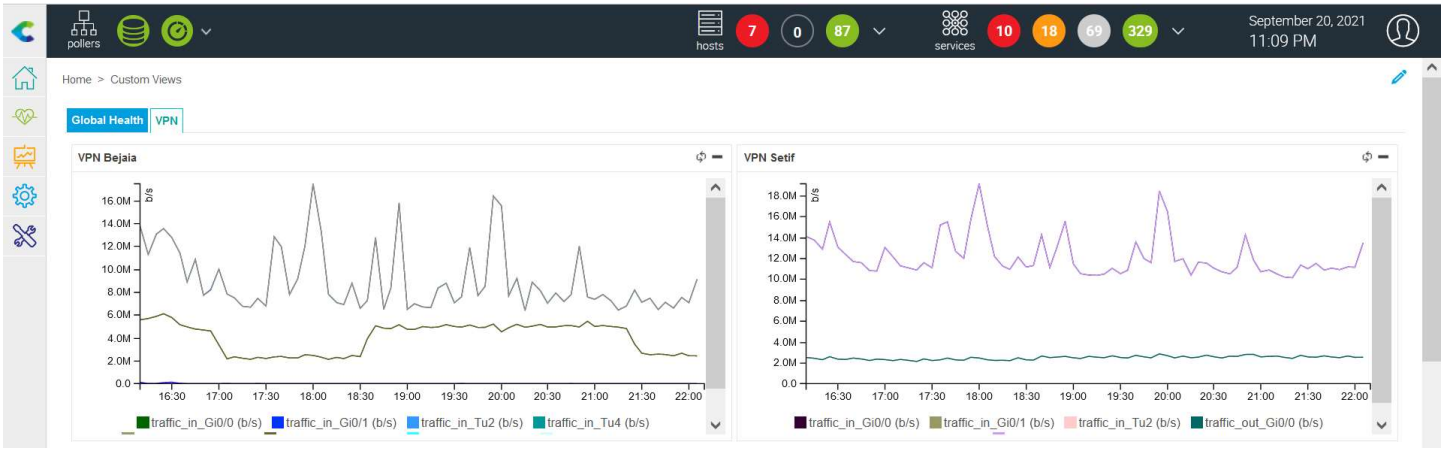


Figure 57 - Centreon Monitoring

Références Bibliographiques

[1] P. ATELIN, Réseaux Informatique - Notions Fondamentales, Editions ENI, 2009.

[2] «Définition VPN,» [En ligne]. Available: https://cours-informatique-gratuit.fr/dictionnaire/vpn/. [Accès le Août 2021].

[3] «Réseau Privé Virtuel VPN,» [En ligne]. Available: https://www.frameip.com/vpn/#1-8211-introduction-au-reseau-prive-virtuel-vpn. [Accès le Septembre 2021].

[4] «Virtualisation des Serveurs,» [En ligne]. Available: https://www.vmware.com. [Accès le Août 2021].

[5] «Netwrix,» [En ligne]. Available: https://www.netwrix.fr. [Accès le Septembre 2021].

[6] «Centron, Supervision Informatique,» [En ligne]. Available: https://www.centreon.com/. [Accès le Juillet 2021].

[7] M. YAZID, *Proposition d'un protocole d'accès au médium dans les réseaux locaux sans fil IEEE 802.11 à fortes contraintes temporelles,* Mémoire de Magistère: Université de Bejaia, 2009.

[8] H. Maroua et T. Vouroumen, *Installation et configuration d'un pare-feu Sophos pour la protection du réseau du CHU de Bejaia,* Mémoire de Master: Université de Bejaia, 2018.

[9] M. PORTNOY, Virtualization Essentials, John Wiley & Sons, 2016.

[10] U. Lakshman et L. Lobo, MPLS Configuration on Cisco IOS Software, Cisco Press, 2010.

[11] Y. Ouzaouit et F. Ait Saghir, Performances Du Mpls Dans Un Réseau Multi Service, Omniscriptum Gmbh & Company Kg, 2014.

[12] A. ERIC, MPLS Traffic Engineering pour l'amélioration des Capacités des connexions IP, Independently Published, 2020.

[13] A. Mauro, P. Valsecchi et K. Novak, Mastering VMware vSphere 6.5, Packt Publishing Ltd, 2017.

[14] «Dell EMC RecoverPoint,» [En ligne]. Available: https://www.delltechnologies.com. [Accès le Juin 2021].

[15] R. MIKES, «What is the Power of RecoverPoint?,» *EMC Proven Professional Knowledge Sharing,* p. 32, 2014.

Résumé

La protection des données est très importante si on veut assurer une continuité des services. Ce modeste travail propose une solution de protection de données basée sur la réplication des VMs critiques, en temps réel, sur un site distant relié au site principal par une liaison VPN MPLS.

En cas d'arrêt d'une VM sur le site principal, une copie distante de cette VM peut être lancée, et les utilisateurs peuvent continuer à travailler sans sentir une différence, grâce à la correction des enregistrements DNS au moment du Failover.

Dans le cas d'un arrêt total du data center principal à la suite d'une catastrophe naturelle, le data center de secours sera lancé, on parle ici d'un Disaster Recovery.

Mots clés : VPN, MPLS, Virtualisation, Serveurs, VMware, VM, RecoverPoint, vSAN, Dell, Réplication, Failover, Protection, Netwrix, Centreon, RPO, RTO.

Abstract

Data protection is very important if we want to ensure continuity of services. This modest work offers a data protection solution based on the replication of critical VMs, in real time, on a remote site linked to the main site by an MPLS VPN link.

If a VM shuts down at the primary site, a remote copy of that VM can be launched, and users can continue working without noticing a difference, it's because of the correction of DNS records at the time of Failover.

In case of a total shutdown of the main data center following a natural disaster, the backup data center will be launched, here, we talk about a Disaster Recovery.

Key Words: VPN, MPLS, Virtualization, Servers, VMware, VM, RecoverPoint, vSAN, Dell, Replication, Failover, Protection, Netwrix, Centreon, RPO, RTO.