République Algérienne Démocratique et Populaire
Ministère de l'Enseignement Supérieur et de la Recherche Scientifique
Université A.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

Étude et mise en place d'une solution de supervision, sauvegarde et réplication réseau et système

Cas d'étude : CEVITAL.

Présenté par :

Mlle : BOUAZOUNE Yasmine & *Mme* : MEHENNI Selma

Soutenu devant le jury composé de :

Présidente :	Mlle : HOCINI Kenza.	Université A. MIRA de Béjaïa.
Examinatrice :	Mme : ZIDANI Ferroudja.	Université A. MIRA de Béjaïa.
Encadrant :	Mme : BELKHIRI Louiza.	Université A. MIRA de Béjaïa.

Promotion 2022/2023

Remerciements

Avant tout, nous tenons à exprimer notre profonde gratitude envers Allah, le clément et le miséricordieux, de nous avoir donné la force et le courage nécessaires pour mener à bien ce modeste travail.

Trouver un stage n'est jamais facile pour un étudiant, c';est pourquoi nous tenons à remercier chaleureusement l'entreprise CEVITAL de nous avoir accueillis pendant ces 2 mois. Nous exprimons notre reconnaissance particulière à Monsieur N. BENOUARETH, notre maître de stage au sein de CEVITAL. Il nous a enseigné de manière très pédagogique dans le domaine des systèmes réseaux et informatiques, et nous le remercions également pour sa disponibilité et la qualité de son encadrement tout au long de notre stage dans l'entreprise.

Nous souhaitons également exprimer notre gratitude envers toute l'équipe de l'entreprise, car chacun d'entre eux a su trouver du temps pour nous aider dans notre mission.

Effectuer notre stage de dernière année au sein de votre entreprise a été un réel plaisir. Grâce à vous, nous avons pu acquérir de nombreuses connaissances et renforcer notre projet professionnel, ce qui constitue un aboutissement de notre parcours universitaire. Nous tenons à exprimer nos sincères remerciements à notre encadrante, Madame L.BELKHIRI, pour le temps q'elle nous a consacré, son écoute attentive et ses conseils tout au long de l'évolution de notre projet.

Nous souhaitons également remercier tous les professeurs qui ont contribué à notre formation.

Nous adressons nos respects les plus sincères à tous les membres du jury pour avoir pris le temps d'examiner notre mémoire.

Enfin, nos remerciements s'adressent également à toutes les personnes de près ou de loin, qui nous ont apporté leur aide et leurs encouragements.

Nous vous sommes profondément reconnaissantes

Dédicace

À mes parents, je suis infiniment reconnaissante pour votre amour inconditionnel,votre dévouement et vos sacrifices. Votre soutien sans faille a été une source de force et de motivation tout au long de ce parcours.Je vous remercie du fond du cœur pour tout ce que vous avez fait pour moi .
Que Dieu vous protège pour moi .

À mes chers frères Aymen,Samy,Ghilas et ma soeur Ritaj

À mon mari, mon meilleur ami et mon plus grand soutien. Ta présence et ton amour inébranlables ont été mes sources d'inspiration.Tu as été là pour moi à chaque étape de ce mémoire, me motivant et me guidant avec ta sagesse et ta bienveillance.
Je t'exprime ma profonde gratitude pour ton soutien indéfectible.

À ma belle nouvelle famille, je vous remercie de m'avoir accueillie à bras ouverts et de m'avoir offert votre soutien et votre amour sincères. Votre acceptation et votre bienveillance m'ont permis de me sentir chez moi et d'avancer sereinement dans mes études.

À ma binôme de mémoire, "Yasmine", notre collaboration, notre travail d'équipe et notre soutien mutuel ont été essentiels à notre réussite. Je suis reconnaissante d'avoir partagé ce voyage avec toi.

Je dédie ce mémoire .

Mehenni Selma

Dédicace

Je dédie ce travail qui n'aurait jamais pu voir le jour sans le soutien indéfectible et sans limite de mes chers parents qui ne cessent de me donner avec amour le nécessaire pour que je puisse arriver à ce que je suis aujourd'hui. Que Dieu vous protège et que la réussite soit toujours à ma portée pour que je puisse vous combler de bonheur. Je dédie aussi ce travail à :

A mes frères et mes sœurs Farid , Massi, Fares, , Siham ,Nassima, Kahina.

A tous ceux que j'aime, à tous ceux qui m'aiment et tous ceux qui me sont chers.

A ma binôme.

A tous ceux qui m'ont aidé durant ma vie universitaire.

Bouazoune Yasmine.

Table des matières

Table des figures

Liste des tableaux

Liste des abréviations

LAN	Local Area Network
PAN	Personal Area Network
MAN	Metropolitan Area Network
WAN	Wide Area Network
OSI	Open Systems Interconnection
TCP/IP	Transmission Control Protocol/Internet Protocol
UDP	User Datagram Protocol
ICMP	Internet Control Message Protocol
ARP	Address Resolution Protocol
RARP	Reverse Address Resolution Protocol
DHCP	Dynamic Host Configuration Protocol
DNS	Domain Name System
SNMP	Simple Network Management Protocol
GNS3	Graphical Network Simulator
VTP	VLAN Trunking Protocol

Introduction générale

Dans un monde en constante évolution, les entreprises modernes sont de plus en plus dépendantes de leurs infrastructures informatiques. Ces infrastructures, regroupant des serveurs, des équipements réseau, des bases de données et des applications critiques, constituent le socle technologique sur lequel repose l'ensemble de l'entreprise. Toute fois, ces environnements technologiques complexes sont sujets à des pannes et à des pertes de données, ce qui peut entraîner des interruptions des services et des conséquences financières importantes.

La surveillance en temps réel des infrastructures est donc essentielle pour détecter rapidement les incidents, les problèmes de performance et les goulots d'étranglement. En surveillant les infrastructures en temps réel, les entreprises peuvent prendre des mesures préventives ou correctives de manière proactive, minimisant ainsi les temps d'arrêt et optimisant les performances.

Cevital dispose déjà d'une solution de supervision, mais celle-ci nécessite des mises à jour régulières et une administration avancée pour rester efficace. Pour répondre aux besoins en constante évolution de notre entreprise, il est primordial de maintenir cette solution à jour en ajoutant de nouvelles fonctionnalités, en améliorant les performances et en renforçant sa capacité à gérer les infrastructures complexes.

Parallèlement, il est crucial de mettre l'accent sur la sauvegarde et la réplication des réseaux et des systèmes au sein des grandes entreprises. La sauvegarde régulière des données de supervision permet de prévenir la perte d'informations critiques et de garantir une reprise après sinistre rapide en cas d'incident majeur. La réplication des configurations assure une disponibilité continue des systèmes et facilite la gestion des environnements distribués.

Dans ce contexte, notre objectif est de mettre à jour et d'améliorer la solution de supervision existante au sein de notre entreprise. Nous visons à réaliser une administration avancée de cette solution en ajoutant des fonctionnalités avancées, en optimisant ses performances et en renforçant sa capacité à gérer les infrastructures complexes. De plus, nous prévoyons la mise en place d'une solution de sauvegarde et de réplication pour les réseaux et les systèmes, afin de garantir la protection et la disponibilité continue des données critiques.

Notre mémoire est structuré en quatre chapitres distincts. Le premier chapitre, intitulé "Présentation de l'organisme d'accueil - CEVITAL Bejaia", se focalise sur la présentation de cet organisme, le contexte du projet et ses objectifs.

Le deuxième chapitre est axé sur " Les Fondements des Systèmes d'exploitation et des Réseaux Informatiques ". Au cours de ce chapitre, nous allons explorer les bases des systèmes d'exploitation et des réseaux informatiques en définissant leurs caractéristiques, leurs classifications, ainsi que leurs objectifs .

Le troisième chapitre, intitulé "La Supervision, la Sauvegarde et la Réplication Informatique", est consacré à une analyse plus approfondie de ces trois éléments. Nous y détaillons leurs objectifs

et nous présentons des outils pertinents pour la supervision, la sauvegarde et la réplication que nous prévoyons d'utiliser.

Le dernier chapitre, " Réalisation et Tests ", se penche sur l'environnement de travail que nous avons mis en place, en fournissant des captures d'écran illustrant les étapes d'installation et de configuration des outils sélectionnés pour la mise en œuvre de notre projet.

Chapitre 1

Présentation de l'organisme d'accueil "CEVITAL de Béjaia", analyse de l'existant, problématique et solution dégagé

Introduction

Au cours de cette partie, nous vous présentons l'organisme d'accueil : Cevital, pour qui nous avons effectué un stage lié à ce projet ; ses fonctions, ses opérations et ses organisations Nous nous concentrons sur le centre informatique de Cevital, ses différents départements et tâches, où nous identifions le problème de notre sujet et nous présentons une solution acceptée à la dernière.

1.1 Partie 1 : présentation de l'entreprise CEVITAL

1.1.1 Création et évolution

Cevital Agro-Industrie est une filiale du groupe Cevital, un conglomérat industriel algérien fondé par Issad Rebrab en 1998 à Béjaïa. L'entreprise s'est spécialisée dans le secteur agro-industriel en investissant dans la production d'huiles végétales, de sucre, de jus de fruits, de produits laitiers, de céréales et d'autres produits alimentaires. Elle possède des fermes agricoles et des usines de transformation à travers l'Algérie. Cevital Agro-Industrie est devenu un acteur majeur de l'industrie agroalimentaire en Algérie, contribuant à l'emploi, au développement régional et à la promotion de l'agriculture et de l'industrie agroalimentaire du pays.

Historique

- 1998 : Création de CEVITAL Agro-industrie ;
- 1999 : Entrée en production de la raffinerie d'huile ;
- 2003 : Entrée en production de la raffinerie de sucre ;
- 2005 : Acquisition de LALLA KHEDIDJA ;
- 2006 : Acquisition de COJEK.
- 2007 : CRÉATION MFG (VERRE PLAT).
- 2008 : CRÉATION DE NUMILOG.
- 2009 : AUGMENTATION DE LA PRODUCTION DE SUCRE DE 1 M T/AN.
- 2013 : OXXO (FRANCE) / ALAS (ESPAGNE).
- 2014 : BRANDT (FRANCE) / AFFERPI (ITALIE) EX LUCCHINI PIOMBINO.

1.1.2 Situation géographique

Le complexe Cevital est situé au nouveau quai du port de Béjaïa, à environ 3 km au sud-ouest de la ville. Il s'étend sur une superficie de 45 000 m2 et est proche de la route nationale N°09. Cette situation géographique avantageuse offre à l'entreprise des avantages économiques significatifs. En effet, sa proximité avec le port et l'aéroport de Béjaïa facilite les échanges commerciaux et les opérations logistiques , voir la figure ci-dessus :

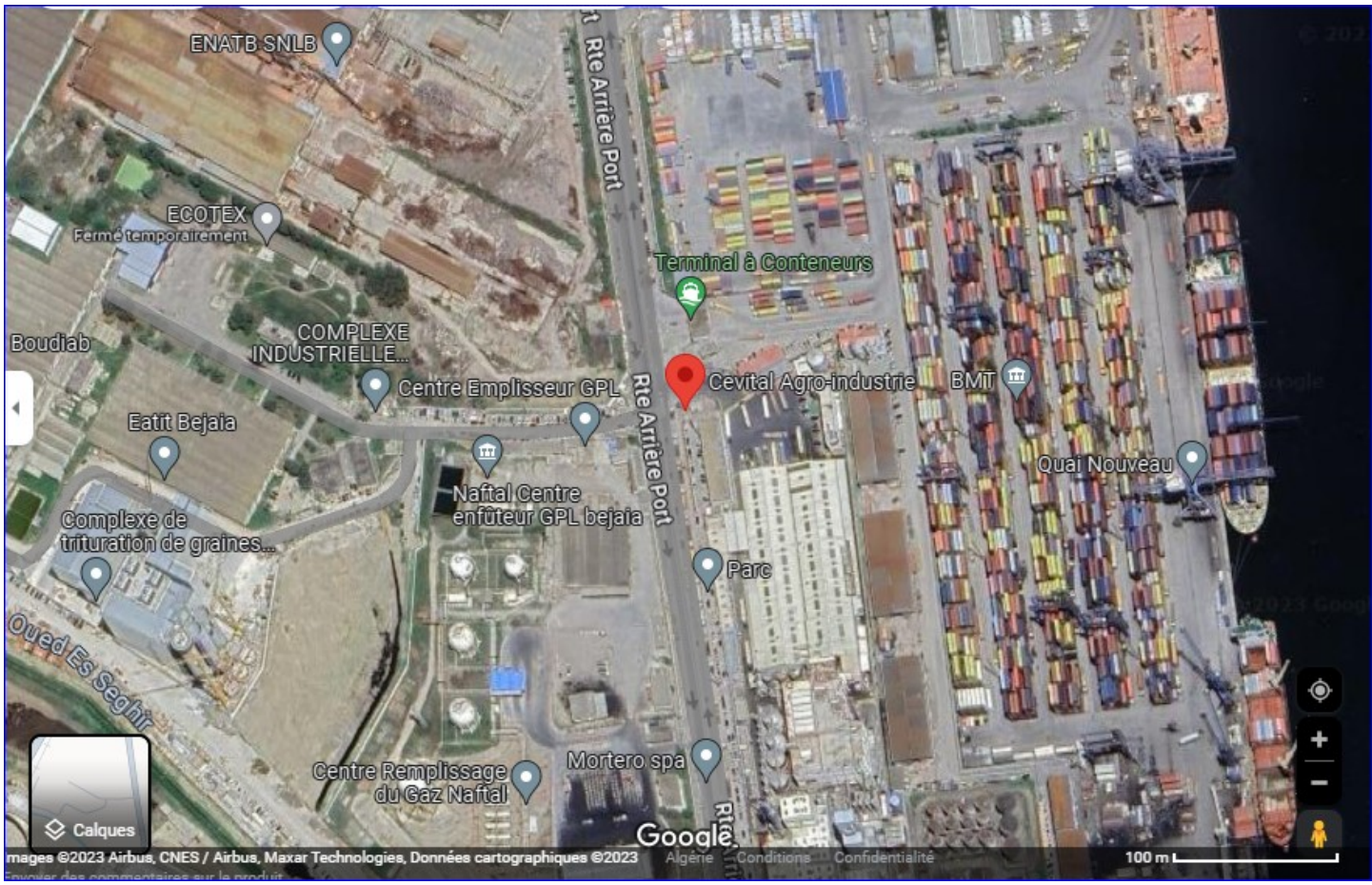


Figure 1.1 – Situation géographique du complexe CEVITAL

1.1.3 Organigramme générale de l'entreprise

Organigramme générale de entreprise est bien expliqué dans la figure ci-dessus :

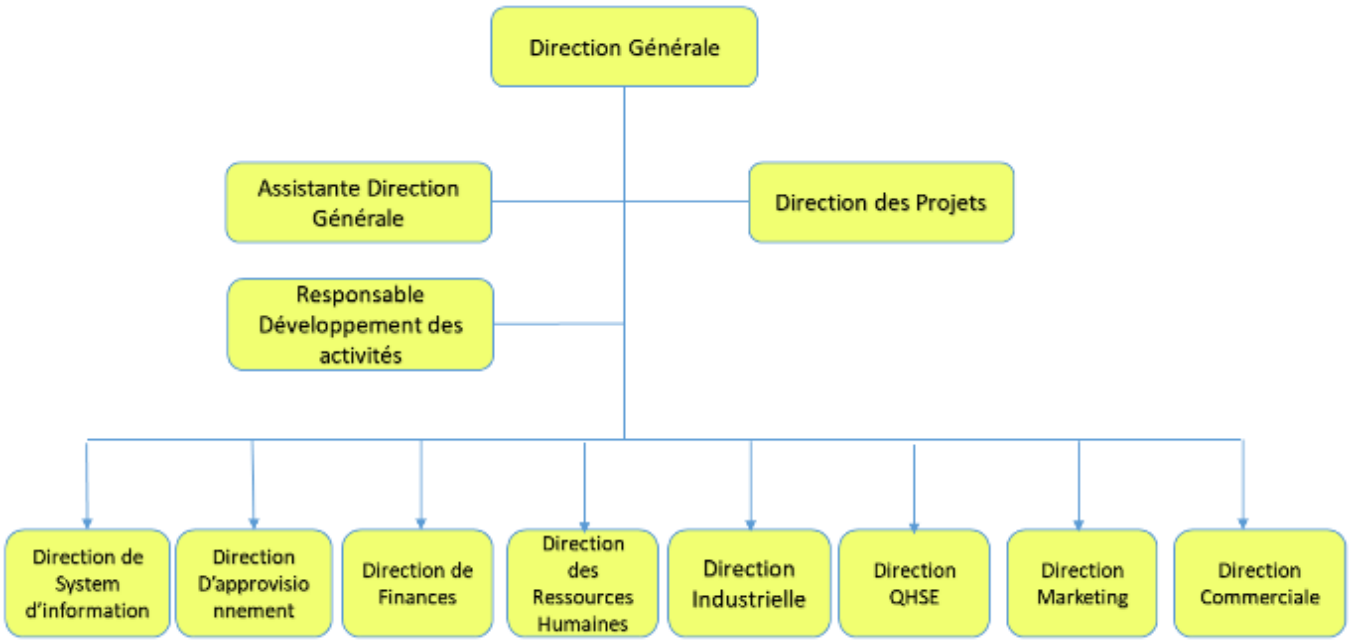


FIGURE 1.2 – Organigramme du Groupe CEVITAL

1.1.4 Organigramme département d'accueil

Notre stage s'est déroulé au sein du Département Système Réseau & Télécom de la Direction des Systèmes d'information. Ce département est responsable de la mise en place des moyens et des technologies de l'information nécessaires pour soutenir et améliorer l'activité, la stratégie et la performance de l'entreprise. Il veille à garantir la cohérence des moyens de communication mis à la disposition des utilisateurs, leur mise à niveau, leur maîtrise technique, ainsi que leur disponibilité et leur fonctionnement continu.

De plus, il définit, dans le cadre des plans pluriannuels, les évolutions nécessaires en fonction des objectifs de l'entreprise et des nouvelles technologies, comme il est montré dans la figure ci-dessus.

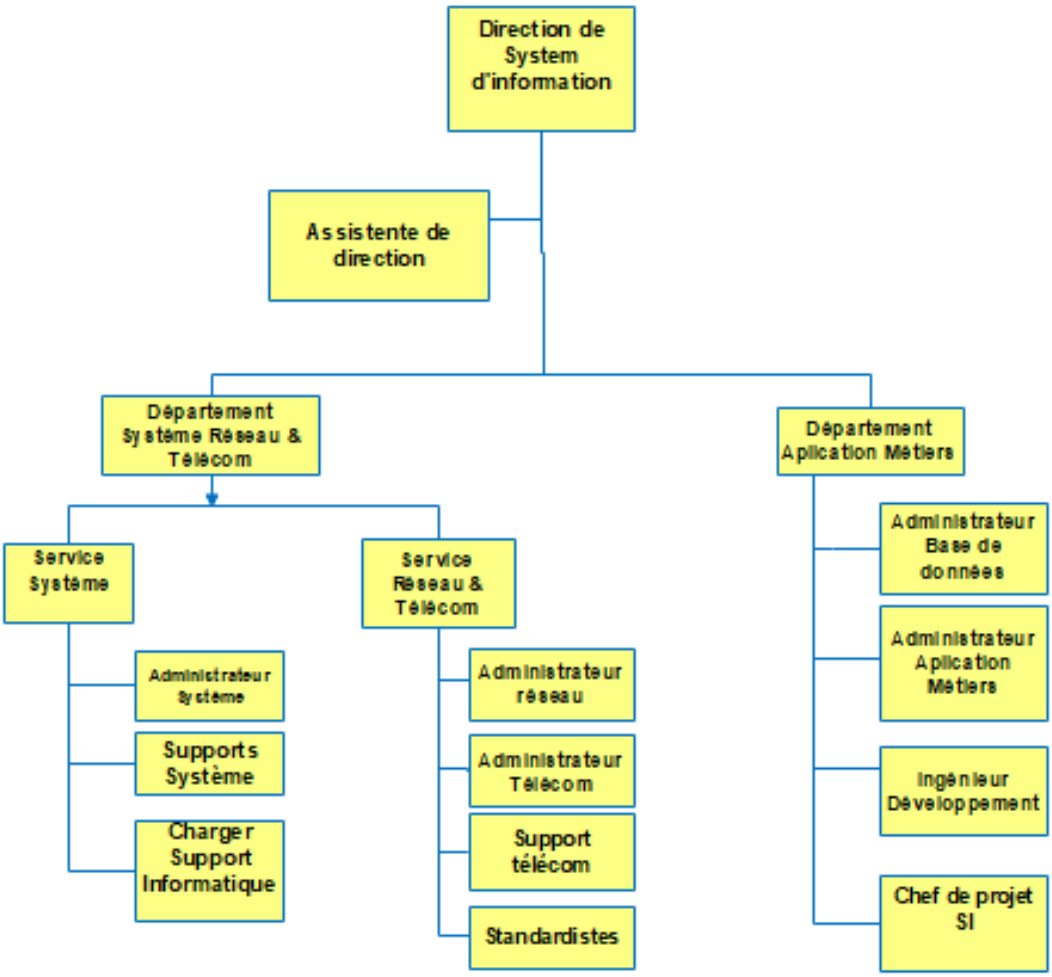


FIGURE 1.3 – Organigramme de la direction système d'information

1.2 Partie 2 :Étude de l'existant

1.2.1 Infrastructure de l'entreprise

CEVITAL Agro-industrie se distingue en tant que premier terminal de déchargement portuaire en Méditerranée grâce à la possession de plusieurs silos portuaires et d'un terminal de déchargement ayant une capacité de 2000 tonnes/heure. De plus, CEVITAL dispose de plusieurs unités de production qui contribuent à ses activités :

- Deux (02) raffineries de sucre .
- Une unité de sucre liquide .
- Une raffinerie d'huile .
- Une margarinerie .
- Une unité de conditionnement d'eau minérale (site de TIZI OUZOU) .
- Une unité de fabrication et de conditionnement de boissons rafraîchissantes (site d'EL Kseur).
- Une conserverie .
- Une unité de fabrication de chaux calcinée.

1.2.2 Architecture global du réseau de Cevital

Cevital dispose d'un réseau interne assez vaste qui assure la liaison entre les divers bâtiments, unités de production et direction du complexe. Nous pouvons le décomposer en plusieurs parties : - Le backbone du réseau.
- Un pare-feu .
- Un DMZ (démilitarized zone) .

Une couverture WIFI, un routeur et un Datacenter (ou sont placés les serveurs de l'entreprise).

Le réseau est composé de plusieurs équipements dont la plupart sont de marque Cisco (Switch, Catalyst, Routeur) interconnectés entre eu grâce à la fibre optique, ou cuivre.

Voici une présentation de l'architecture actuelle du réseau informatique du groupe CEVITAL

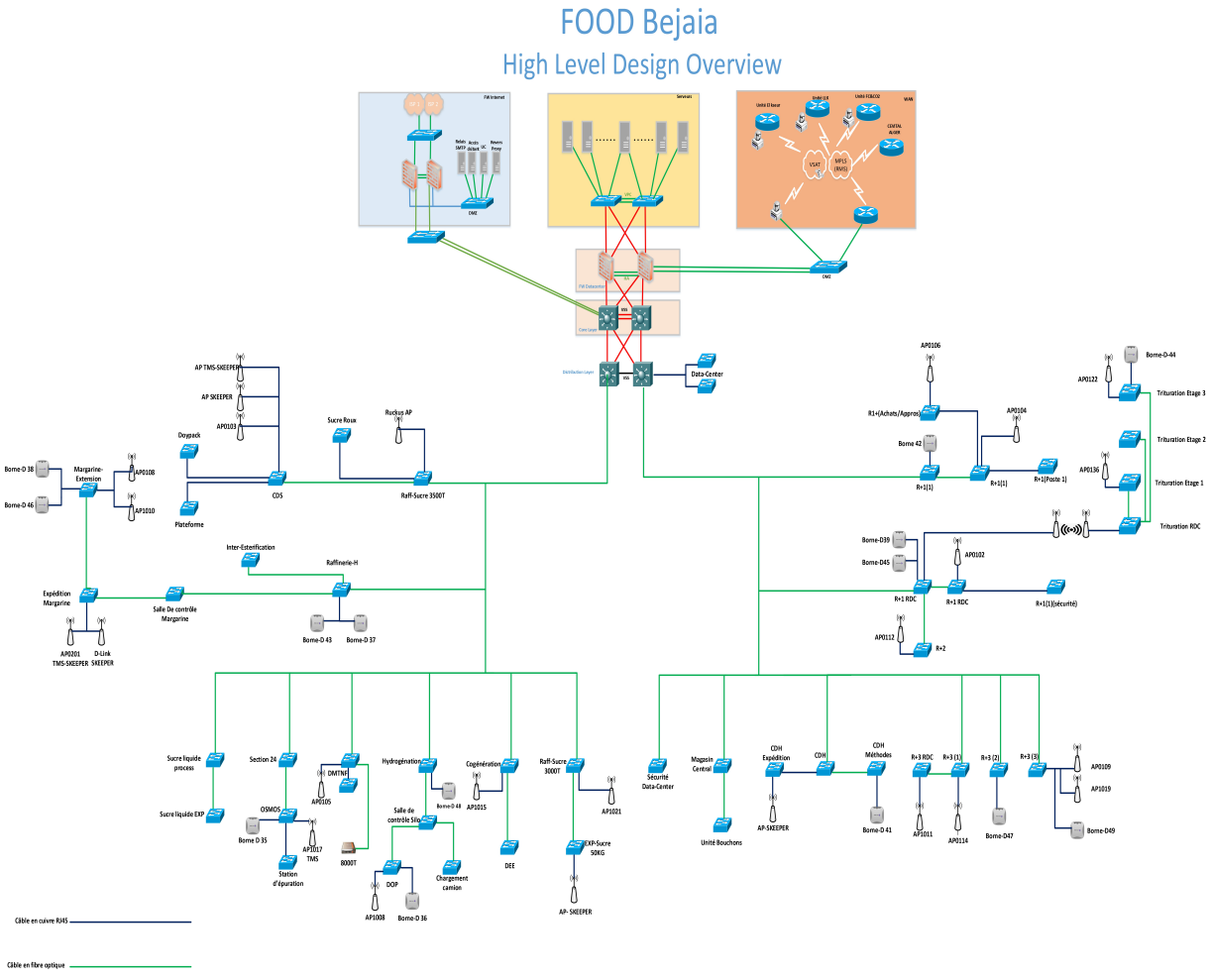


FIGURE 1.4 – L'architecture du réseau informatique de CEVITAL

1.2.3 Présentation du hard et du soft

Matériels utilisé dans l'architecture

A/ **Liaison intra-sites (Architecture LAN) :**

1. **Distribution (Cœur/Backbone) : Cisco Catalyst 4507R**
   Il s'agit de la partie centrale du réseau, responsable du trafic de données le plus important au sein du complexe. Il dispose d'une bande passante considérable.
   Il connecte les différents équipements :switchs d'accès, les pare-feu, les serveurs et le routeur de l'entreprise, qui y sont connectés. Il est chargé du routage entre les VLAN. De plus,
   Il permet l'accès à Internet via le pare-feu et c'est généralement un serveur DHCP ,voir la figure ci-dessus.

FIGURE 1.5 – switch cœur /distributeur

2. **Switch d'accès : Cisco Catalyst 2960X**
   Ils sont connectés au backbone et installés dans les différents bâtiments de l'entreprise,voir la figure ci-dessus.

FIGURE 1.6 – Switch d'accès : Cisco Catalyst 2960X

3. **Switch en cascade : Cisco Catalyst 2960X**

   Les différents Switch de cette couche sont reliés en cascade (entre eux et aux switches d'accès) et fournissent un accès réseaux aux utilisateurs, au sien de ses Switch des VLANs permettent de définir plusieurs sous-réseaux en fonction des départements de l'entreprise,voir la figure ci-dessus .

FIGURE 1.7 – Switch en cascade : Cisco Catalyst 2960X

B/ **Data Center :**

Le data center est une salle sécurisée avec un accès restreint. Seuls les responsables et les techniciens de la DSI (Direction des Systèmes d'information) y sont autorisés. La température est régulée par un système de climatisation et l'alimentation électrique est redondante, garantissant ainsi le bon fonctionnement des équipements qui s'y trouvent. Le data center de Cevital est considéré comme le cœur central du réseau de l'entreprise. On y trouve :

— Les serveurs de l'entreprise.
— Le switch principal.
— Les pare-feu.
— Les routeurs.
— Le standard téléphonique.

voir la figure ci-dessus :

FIGURE 1.8 – Data Center

C/ **Autre équipements :**

1. **Routeur : Cisco 2900**
   voir la figure ci-dessus.

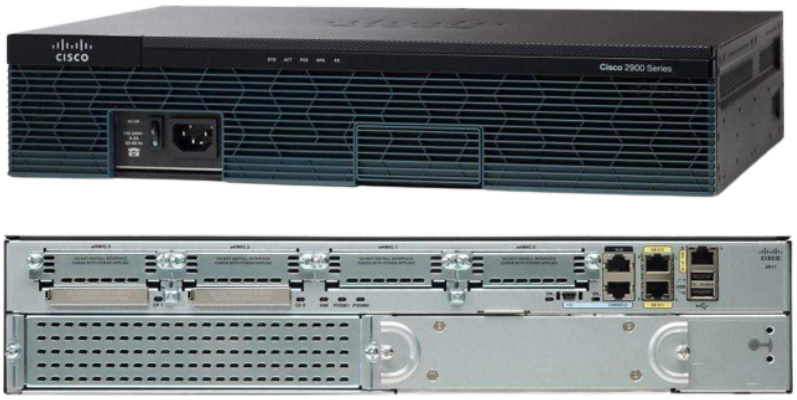


FIGURE 1.9 – Routeur : Cisco 2900

Il gère le routage entre les différents sites de l'entreprise

2. **Pare feu : Fortinet**

   Deux pares-feux sont reliés en redondance et permettant de sécuriser le réseau, d'isoler certaines parties de celui-ci, encadre et sécurise l'accès internet,voir la figure ci-dessus .

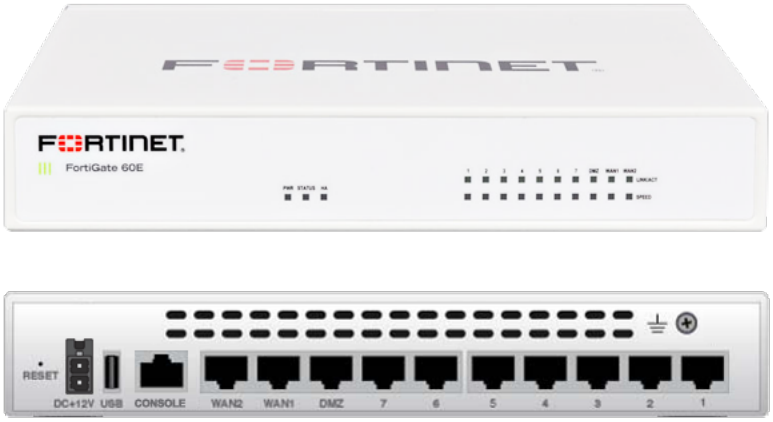


FIGURE 1.10 – Pare feu : Fortinet

3. **Point d'accès WIFI RUCKUS**

L'entreprise possède plusieurs points d'accès WIFI, assurant une couverture réseau sans fil au niveau de certaines parties du complexe ,voir la figure ci-dessus.

FIGURE 1.11 – Point d'accès WIFI RUCKUS

1.2.4 Liaison inter-sites (architecture WAN)

Afin de garantir le partage des ressources et la communication interne au sein de l'entreprise, Cevital met en place des connexions permettant de relier le site de Bejaïa aux différentes annexes de l'entreprise, notamment :

• Une liaison fibre optique point à point entre Bejaïa et Alger.

• Liaison par satellite (Vsat) entre Bejaïa et les sites d'Elkseur (Cojak), site de Tizi-Ouzou (Lala Khadija) et El Khroub.

voir la figure ci-dessus.

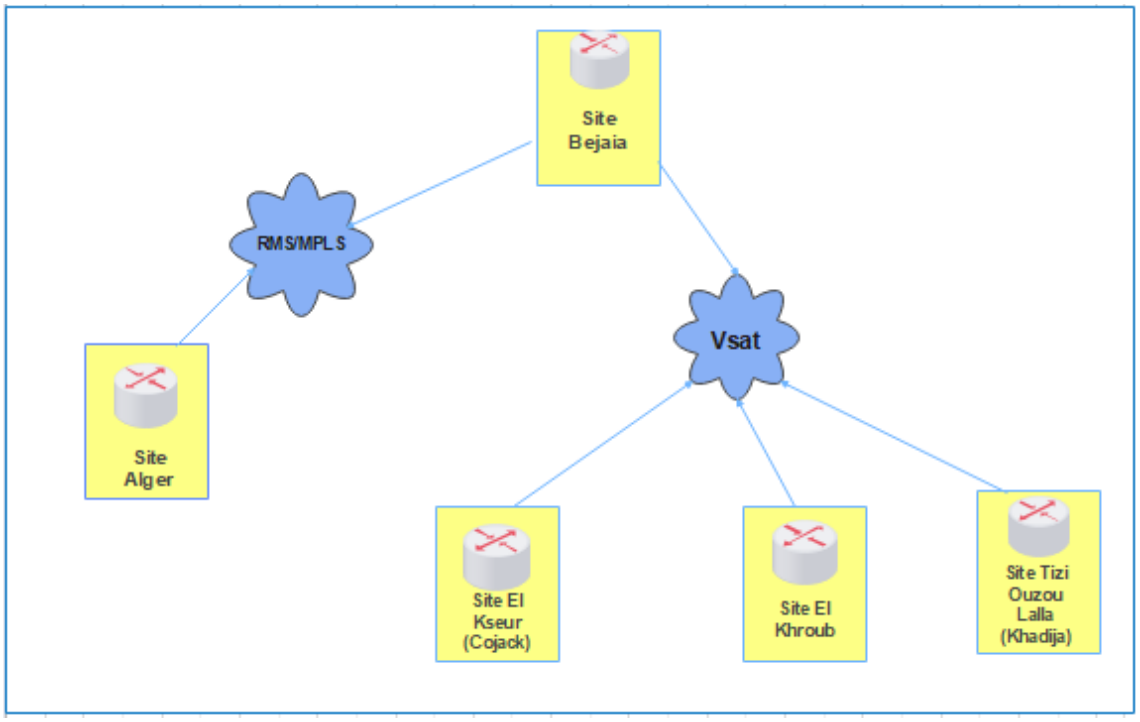


FIGURE 1.12 – Architectures WAN du réseau de Cevital

1.2.5 Analyse du parc informatique

— Cevital dispose de environ 2000 PC HP et ACER répartis à travers les différentes directions de l'entreprise et inter-connecté à un réseau informatique inter-connecté par fibre optique et de câbles à paires torsadés.
— Les systèmes d'exploitation utilisés sur les postes de travail sont Windows et Linux sous différentes distribution. La majorité des PCs est reliée à des imprimantes de plusieurs types (matricielle, laser et à jet d'encre couleur).
— Chaque ordinateur est branché à un onduleur APC de 400 à 1000 VA.
— Tous Les PCs sont dotés d'un anti virus KESPERSKEY.
— Tous les PCs sont connectés à l'internet

1.3 Partie 3 : Contexte du projet à réaliser :

Dans cette partie, nous commençons par exposer le projet à réaliser, puis nous présentons les objectifs issus de l'achèvent de ce dernier. Ensuite, nous dégageons la problématique associée au cahier des charges de notre organisme d'accueil .

1.3.1 Présentation du projet :

L'objectif de ce projet est d'améliorer les performances du réseau de l'entreprise, en mettant l'accent sur deux points phares : la supervision ainsi que la sauvegarde et réplication réseau et système. Notre mission consiste donc à garantir une meilleure exploitation et attribution du réseau et de maintenir la disponibilité et la continuité du système au sein de l'entreprise .

1.3.2 Problématique :

Après quelques mois passés en entreprise, nous avons identifié les problématiques suivantes concernant les solutions de supervision et de sauvegarde utilisées chez Cevital.
Premièrement en ce concerne la supervision nous avons constaté :

Limitations Fonctionnelles de Centreon : Les versions 2.8.26 et 21.10.3 de Centreon présentent des limitations fonctionnelles.

- Ces limitations entravent la collecte efficace des données de supervision.

- Elles impactent l'analyse des performances des systèmes, rendant difficile la gestion et la surveillance des activités Besoin d'évolution des Fonctionnalités.

- Les besoins de l'entreprise évoluent en permanence.

- Les fonctionnalités actuelles de la solution de supervision ne parviennent pas à suivre ce rythme.

Il devient essentiel d'adapter et d'améliorer ces fonctionnalités pour répondre aux nouveaux défis technologiques et aux besoins en expansion de l'entreprise.

Sécurité des Données et Reprise Après Sinistre :
- Les procédures actuelles de sauvegarde et de reprise après sinistre sont-elles adéquates ?
- Quelles sont les mesures en place pour garantir la sécurité des données et la disponibilité en cas de problème majeur ?
- Comment s'assurer que les données critiques sont sauvegardées et récupérables en cas de catastrophe ?
  Gestion des Environnements Distribués : Cevital opère dans un environnement distribué.
- Comment gérer efficacement la supervision et la sauvegarde dans un tel environnement complexe ?
  Quels outils et processus sont nécessaires pour garantir la cohérence et la disponibilité des systèmes à travers les différents sites ?
  Optimisation des Performances et Gestion des Goulots d'Étranglement :
- Comment optimiser les performances des systèmes tout en identifiant et en éliminant les goulots d'étranglement potentiels ?
- Quelles stratégies de surveillance peuvent être mises en place pour assurer une utilisation efficiente des ressources informatiques ?

En second lieu, en ce qui concerne nos solutions de sauvegarde et de réplication, plus précisément la gestion de la sauvegarde et de la réplication de leurs réseaux et systèmes, nous avons repéré un certain nombre de lacunes significatives :

Manque de Planification Stratégique : L'une des principales lacunes réside dans le manque de planification stratégique en ce qui concerne la sauvegarde et la réplication. Il est essentiel de définir des objectifs clairs, des priorités et des stratégies pour garantir la continuité des opérations en cas de défaillance ou de catastrophe. Actuellement, l'absence d'un plan global peut exposer l'entreprise à des risques inutiles.

Sélection d'outils Inadéquats : Nous avons observé que les outils de sauvegarde et de réplication actuellement en place peuvent ne pas répondre pleinement à nos besoins. Il est crucial de s'assurer que les solutions que nous utilisons sont suffisamment flexibles et robustes pour gérer nos environnements informatiques complexes.

Incohérence des Procédures de Sauvegarde : Une autre lacune est l'incohérence des procédures de sauvegarde. Il est impératif d'avoir des procédures de sauvegarde normalisées, régulièrement mises à jour et respectées par l'ensemble de l'entreprise. Cette incohérence peut entraîner des vulnérabilités et des pertes de données potentielles.

Gestion Inefficace des Temps de Récupération : En cas de sinistre, la capacité à récupérer rapidement les données est essentielle. Nous avons remarqué que nos temps de récupération actuels peuvent ne pas être optimaux, ce qui pourrait entraîner des temps d'arrêt plus longs et des perturbations pour nos opérations.

Lack of Testing and Validation : La validation des procédures de sauvegarde et de réplication est essentielle pour garantir qu'elles fonctionnent comme prévu. Cependant, il semble y avoir un manque de tests et de validation réguliers pour les processus de sauvegarde, ce qui peut mettre en péril notre capacité à restaurer les données en cas de besoin.

Difficulté à Répliquer des Environnements Distribués : Dans un environnement complexe et distribué comme le cas de Cevital , la réplication efficace des systèmes peut être un défi. Il est nécessaire de développer des stratégies pour assurer la cohérence des données et la disponibilité continue dans de telles configurations.

En identifiant ces problématiques, nous pouvons élaborer des solutions et des recommandations pour améliorer la supervision des réseaux et systèmes informatiques au sein de Cevital, contribuant ainsi à une meilleure gestion de l'infrastructure technologique de l'entreprise.

1.3.3 Cahier de charge

Notre objectif se divise en deux partie distinctes, pour lesquelles nous suivrons des démarches spécifiques afin de les atteindre.

1 : Partie supervision réseaux et système :

Dans la première partie, nous nous concentrerons sur l'amélioration et l'ajout de nouvelles fonctionnalités à la solution Centreon déjà utilisée chez Cevital. Nous mettrons en place un système de surveillance en temps réel avec des tâches clairement définies, tout en utilisant une administration avancée. L'objectif principal de cette solution de supervision sera de collecter régulièrement les données sur l'état du réseau et des systèmes, puis de les analyser. Notre but est d'accroître la visibilité, d'assurer une gestion proactive des incidents, d'optimiser l'utilisation des ressources et de renforcer la sécurité. En comblant les éventuelles lacunes, nous veillerons à ce que l'infrastructure informatique de notre organisme d'accueil fonctionne de manière efficace et sécurisée.

2 : Partie sauvegarde et réplication réseaux et système :

Dans la seconde partie, concernant la sauvegarde et la réplication des réseaux et des systèmes, notre objectif ultime est de réaliser des sauvegardes régulières et fiables des données, ainsi que de répliquer ces données vers un emplacement distant ou un centre de données secondaire. Nous cherchons à assurer la protection, la disponibilité et la continuité des données et des services critiques de l'entreprise. Ce faisant, nous réduirons les risques de perte de données, permettrons une récupération rapide en cas de panne et renforcerons la sécurité des systèmes.

En résumé, notre objectif principal est de mettre en place une solution de supervision des réseaux et des systèmes pour une meilleure gestion et sécurité, ainsi qu'une solution de sauvegarde et de réplication pour assurer la protection et la disponibilité des données critiques .

1.3.4 Analyse des besoins :

L'objectif de notre travail est de mettre en place deux solutions innovantes :

1. **Une solution de supervision réseau et système :** Cet outil doit être en mesure de surveiller les équipements réseau (switches , routeurs) et systèmes (serveurs et machines virtuelles). Notre objectif est d'assurer une :

— **Surveillance proactive :** La solution de supervision permet une surveillance en temps réel de l'ensemble du réseau et des systèmes de l'entreprise. Cela offre une visibilité accrue des performances et des éventuelles vulnérabilités. Par conséquent, les problèmes potentiels tels que les pannes matérielles, les erreurs de configuration peuvent être détectés précocement. Ainsi, des mesures correctives peuvent être prises rapidement avant qu'ils ne se transforment en problèmes majeurs.

— **Sécurité renforcée :** La supervision constante permet de détecter les activités suspectes ou les tentatives d'intrusion dans le réseau. En surveillant les journaux d'événements et en mettant en place des alertes, les équipes de sécurité peuvent intervenir rapidement pour prévenir les attaques potentielles et renforcer la sécurité globale de l'entreprise.

— **Optimisation des ressources et des coûts :** En supervisant l'utilisation des ressources telles que la bande passante du réseau, la capacité de stockage et la charge du serveur, il devient possible d'identifier les goulets d'étranglement, les inefficacités et les surutilisations. Cette surveillance permet ensuite d'optimiser l'allocation des ressources, de prendre des décisions éclairées en matière d'investissement et de réduction des coûts, et d'éviter les temps d'arrêt coûteux. En conséquence, les coûts liés aux infrastructures sont réduits et l'efficacité opérationnelle est améliorée.

2. **Une solution de sauvegarde et de réplication** : Cette dernière doit être capable de réaliser l'enregistrement et la réplication des données du système afin d'atteindre les objectifs suivants :

— **Protection des données :** La sauvegarde régulière des données critiques assure leur protection contre la perte accidentelle, les erreurs humaines, les attaques malveillantes ou les défaillances matérielles. En cas de problème, les données peuvent être récupérées à partir des sauvegardes, garantissant ainsi leur intégrité et leur disponibilité.

— **Haute disponibilité :** La réplication des systèmes et des données permet d'avoir des copies exactes et synchronisées dans différents emplacements ou serveurs. En cas de défaillance d'un système ou d'une zone géographique, les utilisateurs peuvent être basculés automatiquement vers une autre instance, assurant ainsi une haute disponibilité des services et une continuité des opérations.

— **Continuité des activités :** La mise en place d'une solution de sauvegarde et de réplication contribue à assurer la continuité des activités de l'entreprise. En cas de problème majeur, les données peuvent être récupérées à partir des sauvegardes et les services critiques peuvent être rapidement restaurés, minimisant ainsi l'impact sur les opérations quotidiennes.

— **Réduction des risques :** En répliquant les données sur des sites distants ou dans le cloud, une entreprise réduit les risques de perte de données causés par des événements catastrophiques tels que les incendies, les inondations, les pannes de matériel ou les attaques malveillantes. La redondance des données assure une meilleure résilience et une plus grande fiabilité.

Conclusion

Notre étude approfondie du réseau existant de CEVITAL nous a permis de comprendre son fonctionnement et son importance. Nous avons examiné en détail les équipements, les architectures réseau, ainsi que les besoins et les objectifs en matière de supervision, de sauvegarde et de réplication.

Chapitre 2

Notions de bases sur les systèmes d'exploitations et les réseaux informatiques

Introduction

Les réseaux informatiques et les systèmes d'exploitation jouent un rôle essentiel dans le fonctionnement et la gestion des systèmes informatiques modernes. Dans ce chapitre, nous explorerons les notions de base qui permettent de comprendre ces deux domaines clés de l'informatique.

Dans la première partie on vas définir ce qu'est un réseau informatique, ses objectifs, ses différentes classifications ainsi que les caractéristiques des réseaux. Nous décrivons par la suite les architectures réseaux et les différentes topologies (logiques ou physiques) existantes. Enfin, nous définissons les différentes normes et protocoles de communication.

Dans la deuxième partie, nous définissons les systèmes d'exploitation en présentons un bref historique sur les SE , les différentes classes et architectures des SE ainsi que les services offert par les SE .

2.1 Les réseaux informatiques

2.1.1 Définition

Un réseau informatique est un ensemble d'équipements informatiques (ordinateurs, scanners, imprimantes...) relies entre eux par des moyens de communications (avec câble et sans fil) pour partager des données, ressources matérielles et logicielles et échanger des informations. La figure 2.1 présente un exemple d'un réseau informatique. (17)

FIGURE 2.1 – Réseau informatique

2.1.2 Objectifs

Un ordinateur est une machine permettant de manipuler des données numériques. L'homme, en tant qu'être communiquant, a rapidement compris l'intérêt qu'il pouvait y avoir à relier ces ordinateurs entre-deux afin de pouvoir échanger des informations.

Un réseau informatique peut servir plusieurs buts distincts :(1)

- Le partage de ressources (fichiers, applications ou matériels, connexion à internet, etc.).
- La communication entre processus (entre des ordinateurs industriels par exemple).
- La communication entre personnes (courrier électronique, discussion en direct, etc.) .
- La garantie de l'unicité et de l'universalité de l'accès à l'information (bases de données en réseau).
- Le jeu vidéo multijoueur

2.1.3 La Classification Des Réseaux

On distingue différents types de réseaux selon leur taille, le nombre de machine, leur vitesse de transfert des données ainsi que leur étendue. On distingue généralement quatre catégories de réseaux .(1)

1. **Réseau personnel (PAN ou Personal Area Network) :**
   Petit réseau de quelques mètres d'étendus, permettant l'interconnexion de machines personnelles : Pc portables, mobile téléphonique, agenda électronique, etc.

2. **Réseau local (LAN ou Local Area Network) :**
   Un réseau local, désigne une zone géographique, plus au moins délimitée par l'existence d'un mur ou d'une barrière plus au moins définie et qui sert à délimiter physiquement une étendu. Un LAN un réseau dont l'étendu s'arrête à partir d'un emplacement défini.

3. **Réseau métropolitain (MAN ou Metropolitan Area Network) :**
   Définit un type de réseau qui s'étend à une métropole ou à une zone géographique qui s'en approche, bien moins étendu qu'un WAN.
   Les MAN sont souvent utilisés par les fournisseur d'accès Internet pour relier les centres de données ou par les administrateur/université qui ont besoin de connecter des sites géographiquement situé dans un périmètre relativement restreint.
   (16)
4. **Réseau étendu (WAN ou Wide Area Network) :**
   Par opposition au LAN, est l'ensemble des équipements sur lesquels l'entreprise n'a pas un contrôle direct en tant qu'entité. D'un point de vue géographique, l'acronyme WAN désigne les réseaux des opérateurs internet, qui sont bien plus étendus que les réseaux d'entreprise. Il peut s'étendre entre des villes, des pays voire des continent, voir la figure ci-dessus.

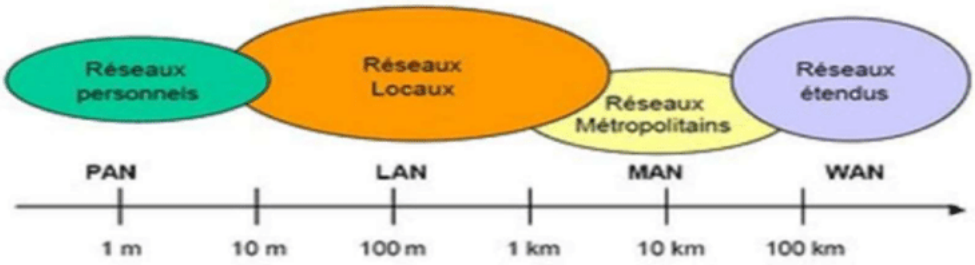


Figure 2.2 – Types des réseaux selon étendu.

2.1.4 Les architectures des Réseaux

Il existe deux types d'architecture de réseaux : Architecture Client/serveur et architecture poste à poste(paire à paire).(8)

1. **Architecture Client/serveur :**
   L'architecture client/serveur (figure 2.3) désigne un modèle de communication entre plusieurs ordinateurs d'un réseau, Elle distingue plusieurs postes clients qui communiquent avec un serveur (une machine généralement très puissante en termes de capacités de traitement ou de stockage) qui leur fournit des services.(8)
   Ces services sont des programmes fournissant des données telles que l'heure, des fichiers, des connexions, etc. Les services sont exploités par des programmes appelés programmes clients s'exécutant sur les machines clientes.
   voir la figure ci-dessus.

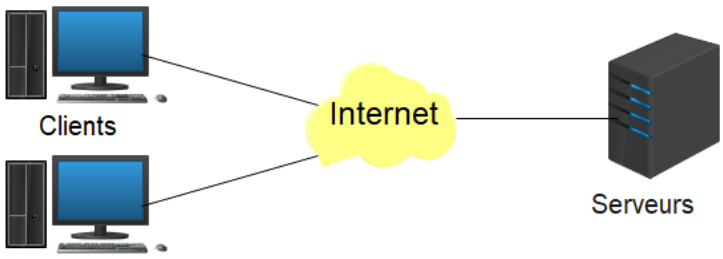


FIGURE 2.3 – Architecture client/serveur .

2. **Architecture poste à poste (égal à égal)**
   Inversement à une architecture de réseau de type client/serveur, il n'y a pas de serveur dédié. Ainsi, chaque ordinateur dans un tel réseau joue à la fois le rôle de serveur et de client. Cela indique notamment que chacun des ordinateurs du réseau est libre de partager ses ressources.
   Les réseaux poste à poste (figure 2.4) ne nécessitent pas les mêmes niveaux de performance et de sécurité que les logiciels réseaux pour serveurs dédiés ,voir la figure ci-dessus .

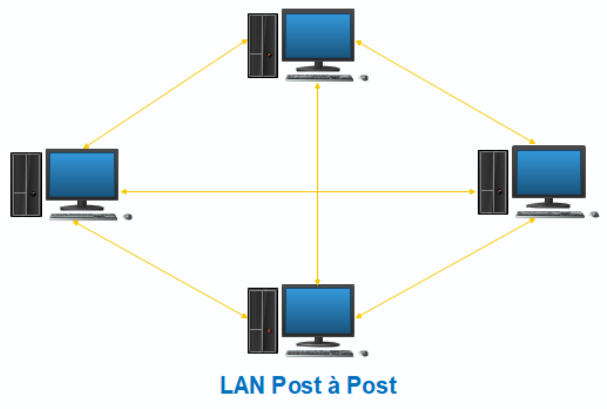


FIGURE 2.4 – Architecture poste à poste

Dans un réseau poste à poste typique, il n'y a pas d'administrateur. Chaque utilisateur administre son propre poste. D'autre part tous les utilisateurs peuvent partager leurs ressources comme ils le souhaitent. (17)

2.1.5 Topologies des Réseaux

La manière dont sont interconnectées les machines est appelée « topologie ». On distingue la topologie physique (la configuration spatiale, visible du réseau) de la topologie logique . (16)

1. **La topologie Logique**

   Elle représente la façon dont les données transitent dans les lignes de communication. Les topologies logiques les plus courantes sont Ethernet,Token-ring et FDDI.

2. **La topologie physique**

   Elle désigne la manière dont les équipements sont interconnectés entre eux. Dans cette topologie, il y a cinq grandes classes qui sont : topologie en bus, anneau, étoile, arbre, anneau et topologie maillée.

   (a) **Topologie En bus :**

   La topologie en bus (support linéaire) comme le montre la figure 2.5 repose sur un câblage, sur lequel viennent se connecter des nœuds (postes de travail, équipements d'interconnexion, périphériques). Il s'agit d'un support multipoints. Le câble est l'unique élément matériel constituant le réseau et seuls les nœuds génèrent les signaux,voir la figure ci-dessus.(14)

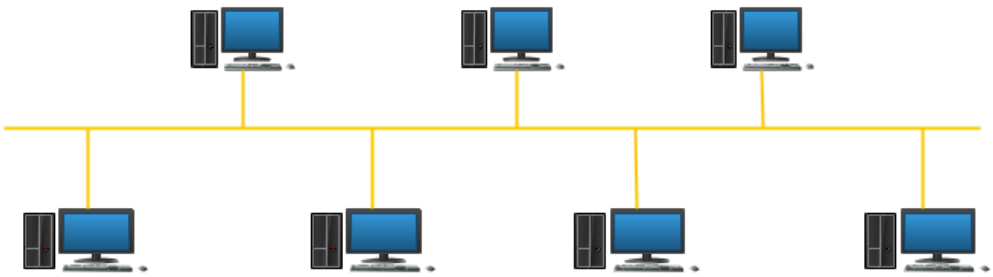


FIGURE 2.5 – Topologie en Bus.

La topologie en bus ne nécessite pas une grande quantité de câbles ni de points centraux, par contre son inconvénient majeur est dû au fait que si le bus est coupé, les stations ne pourront pas s'échanger des informations sur le réseau.

(b) **Topologie En étoile :**

La topologie en étoile repose, quant à elle, sur des matériels actifs. Un matériel actif remet en forme les signaux et les régénère.

Ces points centraux sont appelés des concentrateurs (hubs). Il est possible de créer une structure hiérarchique en constituant un nombre limité de niveaux. (20)

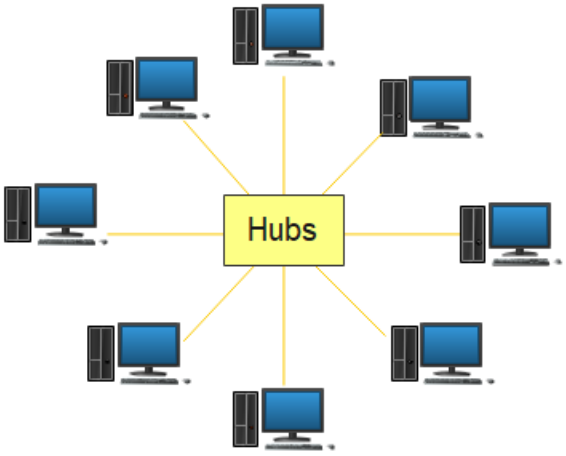


FIGURE 2.6 – Topologie en étoile.

(c) **Topologie En anneau :**

Cette topologie repose sur une boucle fermée, constituée de liaisons point à point entre périphérique. Les trames transitent par chaque noeud qui se comporte comme un répéteur (élément actif). Les concentrateurs en anneau permettent l'insertion de stations dans un réseau. La figure 1.7 montre la topologie en Anneau.(14)

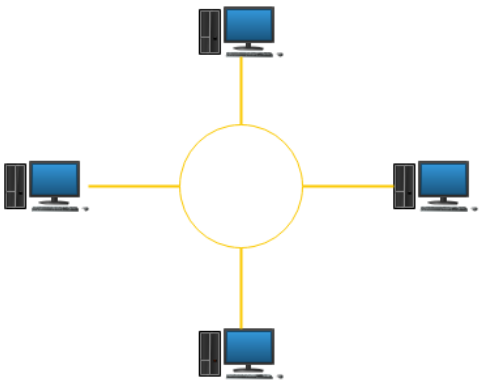


FIGURE 2.7 – Topologie en anneau.

(d) **Topologie en Arbre :**
Dans cette architecture, les postes sont reliés entre eux de manière hiérarchique, à l'aide de concentrateurs cascadables. La figure 2.8 montre la topologie en Arbre.(16)

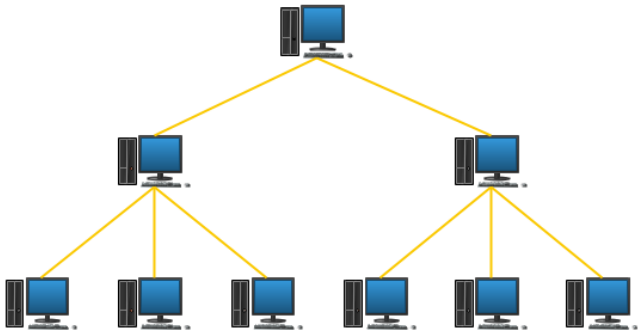


FIGURE 2.8 – Topologie en Arbre .

2.1.6 Les normes de communication réseau

Un réseau informatique permet de partager des données et fichiers ou des périphériques entre plusieurs ordinateurs.

La transmission d'information entre deux programmes informatiques sur deux machines différentes passe par deux modèles :

— Le modèle OSI

— Le modèle TCP/IP.

1. **Le modèle OSI**
L'ISO (International Organization for Standardization) a développé, en 1978. le modèle OSI (Open Systems Interconnection) qui présente une structure en couche. Chaque couche fourni des services à la couche supérieure et utilise les services de la couche inférieure.
Le modèle OSI est basée sur sept couches, la plus haute présente les programmes d'applications tandis que la plus basse présente l'électronique et les mécanismes de transmission des bits sur un support de transmission,voir la figure ci-dessus. (10)

Le rôle de chacune des couches de la figure 2.9 est :(16)

(a) **Couche Physique :**
Elle a pour rôle la transmission bit à bit sur le support entre l'émetteur et le récepteur ,leur encodage et la synchronisation entre deux équipements réseau .

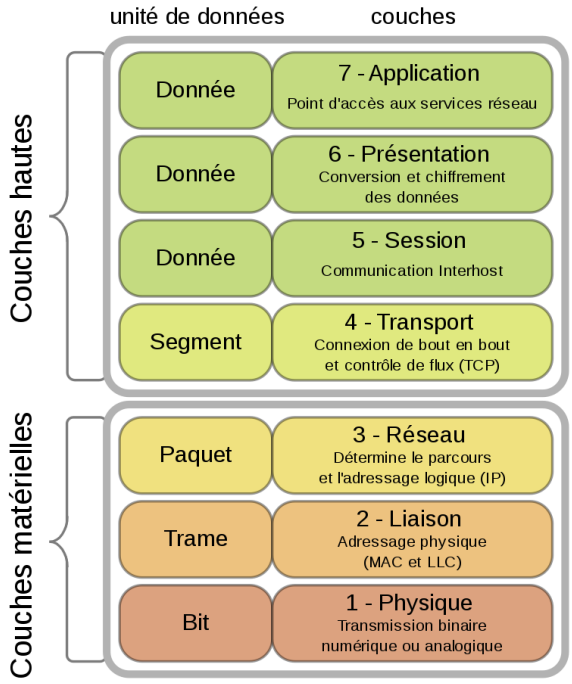


FIGURE 2.9 – Modèle OSI

(b) **La couche liaison :**

S'occupe de la transmission d'un flux de bits entre deux ordinateurs, par l'intermédiaire d'une liaison point à point ou multi-point.

(c) **La couche réseau :**

Permet d'acheminer correctement les paquets d'informations jusqu''a l'utilisateur final. Pour aller de l'émetteur au récepteur, il faut passer par des noeuds de transfert intermédiaire inter-connectant deux ou plusieurs réseaux. Cette couche assure trois fonctionnalités principales :

— Le contrôle de flux,
— Le routage
— L'adressage

(d) **La couche transport :**

Permet de gérer la communication entre deux programmes, deux processus. Les deux protocoles de cette couche sont les protocoles TCP et UDP. Elle est la dernière couche de contrôle des informations. Elle doit assurer aux couches supérieures un transfert fiable quelle que soit la qualité du sous-réseau de transport utilisé.(10)

(e) **La couche session :**

Comme son nom l'indique, permet de gérer les connexions et déconnexions et la synchronisation entre deux processus.

(f) **La couche présentation :**

Elle s'occupe du codage des information ,quelque soient les modes de représentation interne des machines et dans le réseau. Elle se charge également de la compression de données et de leur manipulation (chiffrement/ déchiffrement) .(10)

(g) **La couche Application :**
Cette couche est le point de contact entre l'utilisateur et le réseau, c'est donc elle qui apporte à l'utilisateur les services de base offerts par le réseau, comme par exemple le transfert de fichiers, la messagerie, etc.

2. Le modèle TCP / IP

Le modèle TCP/IP est plus simple qu'OSI, avec seulement quatre couches : Accès au réseau, Internet, transport et application. La différence avec OSI est simplement que certaines couches ont été fusionnées. La couche accès au réseau de TCP/IP regroupe notamment les couches physiques et liaison d'OSI. De même, la couche application de TCP/IP regroupe les couches session, application et présentation d'OSI,voir la figure ci-dessus. (2)

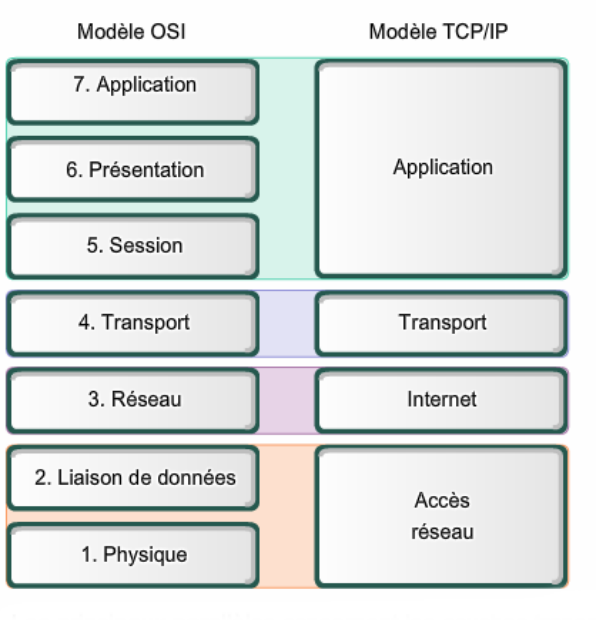


FIGURE 2.10 – le Modèle TCP/IP

2.1.7 Les Protocoles Réseaux

Un protocole de communication est un ensemble de règles qui rendent les communications possibles, ils définissent une sorte de lagunage commun que les intervenants utilisent pour se trouver, se connecter l'un a l'autre et y transporter des informations. (23)

IP (Internet Protocol)

L'IP est un protocole essentiel au sein de la famille TCP/IP, responsable de l'acheminement des paquets. Son objectif principal est d'assurer une livraison optimisée des données, sans établir de connexion préalable. Il est important de souligner que cette optimisation ne garantit pas la livraison des paquets à leur destination finale ni leur réception dans l'ordre d'envoi. Ce sont les protocoles de niveau supérieur qui sont chargés de gérer le contenu des paquets IP et leur ordre de réception.

Le protocole IP fonctionne en mode non connecté, ce qui signifie que les paquets sont acheminés de manière autonome sous forme de datagrammes, sans garantie de livraison.

TCP (Transmission Control Protocol)

TCP est un protocole de niveau supérieur qui assure la sécurité et la fiabilité de la transmission des paquets sur Internet. Il garantit l'ordre et la remise des paquets, vérifie leur intégrité et retransmet les paquets perdus ou altérés. Cette fiabilité en fait un choix adapté pour les applications client-serveur et les services critiques tels que le courrier électronique. Cependant, cette fiabilité a un coût en termes d'utilisation de ressources réseau. Les en-têtes TCP nécessitent des bits supplémentaires pour la mise en séquence et un total de contrôle pour garantir la fiabilité. De plus, les accusés de réception (ACK) génèrent une activité réseau qui réduit le débit. Pour atténuer cet impact, les hôtes n'envoient généralement des ACK que pour certains segments ou lorsque le délai d'attente expire. En fin de compte, TCP assure la livraison fiable des données dans l'ordre sur une connexion entre deux machines du réseau.(2)

UDP (User Datagram Protocol)

UDP est un protocole de la couche transport du modèle TCP/IP. Contrairement à TCP, il n'établit pas de connexion préalable entre les machines. Il transporte des datagrammes de manière indépendante, chaque datagramme étant considéré comme une entité isolée et autonome, contenant toutes les informations nécessaires à son acheminement. UDP ne garantit pas le chemin, le temps ou la séquentialité de la livraison des messages, et ne fournit pas d'accusés de réception. De plus, les paquets peuvent être retransmis plusieurs fois en raison des temporisateurs réseau. L'en-tête UDP contient des informations limitées telles que les adresses source et destination, la longueur du datagramme, et une zone de contrôle d'erreurs. Pour envoyer un datagramme, l'adresse et le numéro de port de destination doivent être spécifiés à l'aide des primitives appropriées, et ces informations sont généralement disponibles dans les tables système. (13)

ICMP (Internet Control Message Protocol)

Le protocole IP ne garantit pas la bonne réception des paquets par leur destinataire. Les paquets sont transmis de passerelle en passerelle jusqu'à ce qu'ils atteignent une qui puisse les délivrer directement. Cependant, en cas d'événements anormaux tels qu'une congestion du réseau ou une indisponibilité d'une machine, il est nécessaire d'informer l'émetteur du paquet de la situation. C'est

là qu'intervient ICMP, un mécanisme de contrôle des erreurs au niveau IP, également connu sous le nom de "protocole de maintenance". ICMP permet aux systèmes d'un réseau IP de partager des informations sur l'état et les erreurs.

La commande "Ping" utilise des paquets ICMP d'écho et de réponse pour déterminer si un système IP donné fonctionne sur un réseau. C'est pourquoi l'outil "Ping" est utilisé pour diagnostiquer les problèmes au niveau d'un réseau IP ou des routeurs.(13)

ARP (Address Resolution Protocol)

Le protocole Address Resolution Protocol (ARP) est utilisé pour associer une adresse IP à une adresse physique (adresse MAC) d'un appareil. Voici un résumé de son fonctionnement :

Lorsqu'une station "A" souhaite envoyer un paquet IP à une station "B" sur le même réseau local, mais ne connaît pas son adresse MAC, elle envoie une requête ARP. Cette requête contient l'adresse IP de "A" et une adresse MAC inconnue pour "B". La requête est diffusée à toutes les stations du réseau local.(23)

La station "B" qui reconnaît son adresse IP répond avec une réponse ARP contenant son adresse MAC. La réponse est envoyée à la station "A".

Après réception de la réponse, la station "A" peut envoyer ses paquets IP avec l'adresse MAC correcte pour la station "B" et met à jour sa table ARP. Cela évite de refaire une requête ARP la prochaine fois. Cependant, il est recommandé de vérifier régulièrement la table ARP en refaisant des requêtes ARP, car le réseau peut changer et les adresses MAC peuvent être modifiées.

RARP (Reverse Address Resolution Protocol)

Le protocole Reverse Address Resolution Protocol (RARP) est moins répandu et sert principalement à obtenir l'adresse IP d'une station de travail sans disque dur à partir de son adresse MAC. Cela fonctionne en utilisant une table de correspondance stockée dans une passerelle du réseau local (LAN).

Lorsqu'une station de travail souhaite connaître son adresse IP, elle envoie une requête RARP contenant son adresse MAC à la passerelle. La passerelle répond ensuite avec l'adresse IP correspondante.

En résumé, le protocole RARP est utilisé dans des cas spécifiques où les stations de travail sans disque dur doivent obtenir leur adresse IP en utilisant une table de correspondance stockée dans une passerelle.(23)

DHCP (Dynamic Host Configuration Protocol)

Le protocole DHCP permet à un ordinateur connecté à un réseau local d'obtenir automatiquement sa configuration IP de manière dynamique. Son objectif principal est de simplifier l'administration d'un réseau. Le DHCP fonctionne selon un modèle client-serveur, où un serveur détient la politique d'attribution des configurations IP et envoie une configuration spécifique pour une durée déterminée à un client (généralement une machine qui vient de démarrer). Le client reçoit alors les informations suivantes : une adresse IP, un masque réseau, une passerelle par défaut et un ou plusieurs serveurs DNS.

Le serveur DHCP joue un rôle central dans toutes les requêtes DHCP, recevant ces requêtes et y répondant. Il doit également avoir une adresse IP fixe. Dans un réseau, il ne peut y avoir qu'une seule machine avec une adresse IP fixe, et c'est le serveur DHCP.(13)

DNS (Domain Name System)

Le DNS (Domain Name System) est un service qui permet de traduire les noms de domaine en adresses IP. Au lieu de devoir connaître et entrer des adresses IP numériques, les utilisateurs peuvent simplement se souvenir des noms de domaine des sites web. Cela facilite l'accès et l'utilisation d'Internet, car il est plus facile d'apprendre et de retenir des noms de domaine que des adresses IP. Le DNS joue un rôle clé dans la convivialité et l'accessibilité d'Internet.(19)

2.2 Les systèmes d'exploitation.

2.2.1 Définition.

Les systèmes d'exploitation sont des logiciels essentiels qui gèrent les ressources matérielles et logicielles d'un ordinateur ou d'un appareil électronique. Ils fournissent une interface entre l'utilisateur et le matériel, permettant ainsi aux utilisateurs d'interagir avec l'ordinateur et d'exécuter des applications. Les systèmes d'exploitation assurent la gestion des fichiers, la planification des tâches, la gestion de la mémoire, la gestion des périphériques, la sécurité et la protection des données. Ils permettent également l'exécution simultanée de plusieurs applications en partageant les ressources disponibles. Les systèmes d'exploitation les plus couramment utilisés sont Windows, macOS, Linux, Android et iOS.(11)

2.2.2 Historique

Les systèmes d'exploitation ont connu une évolution significative depuis leur apparition dans les années 1950. Au fil des décennies, de nouvelles fonctionnalités et innovations ont été introduites, transformant la manière dont les utilisateurs interagissent avec les ordinateurs. Voici un aperçu de l'historique des systèmes d'exploitation :
(**?**)

- Les premiers systèmes d'exploitation ont été développés dans les années 1950 pour simplifier la programmation des ordinateurs.
- Dans les années 1960, la multiprogrammation a été introduite, permettant l'exécution simultanée de plusieurs programmes.
- Les années 1970 ont vu l'émergence de systèmes d'exploitation majeurs tels qu'UNIX et MS-DOS.
- Les années 1980 ont été marquées par l'introduction des interfaces graphiques, facilitant l'interaction avec les ordinateurs.
- Depuis le début des années 2000, les systèmes d'exploitation mobiles, tels qu'Android et iOS, ont dominé le marché.

2.2.3 Les types de SE

Les systèmes d'exploitation peuvent être classés en différents types en fonction de divers critères. Voici un tableau qui représente les principaux types de systèmes d'exploitation selon différentes diversités : (11)

Type		Caractéristique
Selon l'architecture	• Systèmes d'exploitation monopostes .	• Conçus pour les ordinateurs personnels avec un seul utilisateur. Ils offrent une interface conviviale.
	• Systèmes d'exploitation multipostes .	• Permettent à plusieurs utilisateurs d'accéder simultanément au système avec leurs propres ressources.
Selon le domain d'application	• Systèmes d'exploitation de bureau .	• Destinés aux ordinateurs personnels avec une interface graphique conviviale.
	• Systèmes d'exploitation mobiles .	• Conçus pour les smartphones et les tablettes avec des fonctionnalités adaptées à la mobilité et à l'utilisation tactile.
	• Systèmes d'exploitation en temps réel .	• Utilisés dans des applications nécessitant des réponses en temps réel.
	• Systèmes d'exploitation embarqués .	• Optimisés pour les dispositifs embarqués tels que les appareils médicaux et les systèmes de navigation.
Selon le mode de fonctionnement	• Systèmes d'exploitation mono-utilisateur .	• Conçus pour un seul utilisateur à la fois.
	• Systèmes d'exploitation multi-utilisateurs .	• Permettent à plusieurs utilisateurs d'accéder simultanément au système et de partager les ressources.

FIGURE 2.11 – Les Types de SE

2.2.4 Architecture de SE

L'architecture des systèmes d'exploitation (SE) fait référence à la structure interne et à l'organisation des différents composants qui constituent un SE. Il existe différentes architectures de systèmes d'exploitation, chacune avec ses propres caractéristiques et fonctionnalités. Voici quelques-unes des architectures de SE les plus courantes . (9)

1. **Architecture monolithique :**
   Toutes les fonctionnalités du système d'exploitation sont regroupées en un seul noyau monolithique qui gère toutes les opérations système.
   Exemples : Unix, Linux, Windows .
2. **Architecture en couches :**
   Le système d'exploitation est divisé en plusieurs couches distinctes, chaque couche étant responsable d'un ensemble spécifique de fonctionnalités. Les couches communiquent entre elles via des interfaces définies.
3. **Architecture à micro-noyau (microkernel) :**
   Le noyau fournit uniquement les fonctionnalités essentielles, telles que la gestion des processus, de la mémoire et la communication interprocessus. Les fonctionnalités non essentielles sont déplacées en dehors du noyau et implémentées en tant que processus utilisateur.
   Exemples : QNX, MINIX.
4. **Machines virtuelles :**
   Les systèmes d'exploitation basés sur des machines virtuelles fournissent une couche d'abstraction entre le matériel et les applications. Les programmes s'exécutent dans une machine virtuelle qui simule une machine physique.
   Exemples : Java Virtual Machine (JVM), .NET Framework Common Language Runtime (CLR).
5. **Architecture orientée service :**

Les systèmes d'exploitation distribués utilisent une architecture orientée service, où des services autonomes interopérables communiquent via des protocoles standardisés. Les services peuvent résider sur différents ordinateurs pour fournir les fonctionnalités du système d'exploitation.
Exemple : Amoeba.

2.2.5 Les services offerts par les SE

Les systèmes d'exploitation (SE) offrent une variété de services pour les utilisateurs et les applications qui s'exécutent sur un ordinateur. Voici quelques-uns des services les plus courants que les systèmes d'exploitation offrent : (15)

1- Gestion des fichiers.

2- Exécution des programmes.

3- Opération d'Entrées/sorties.

4- Communication.

5- Détection des erreurs.

6- Allocation des ressources.

7- Protection et sécurité.

Conclusion

Ce chapitre nous a permis de divulguer les notions et les aspects élémentaires des systèmes d'exploitation et réseaux informatiques, et comme aussi nous a aidé à distinguer l'aspect physique et le fonctionnement logique du réseau par rapport aux protocoles qui les mettent en bon état de fonction.

Chapitre 3

La supervision, la sauvegarde et la réplication Informatique

Introduction

La gestion efficace des réseaux et des systèmes informatiques repose sur plusieurs aspects clés, notamment la supervision, la sauvegarde et la réplication. Dans ce chapitre, nous allons explorer ces domaines importants et examiner en détail leurs définitions, objectifs, principes et mécanismes.

La supervision, ou monitoring, joue un rôle essentiel dans la surveillance en temps réel des équipements, des applications et des services informatiques. Nous commencerons par définir la supervision et expliquer son objectif. Nous explorerons également les principes fondamentaux de la supervision et présenterons le protocole SNMP (Simple Network Management Protocol), largement utilisé dans ce contexte.

Ensuite, nous aborderons la sauvegarde, également connue sous le nom de "Backup". Nous examinerons sa définition et expliquerons son principe de fonctionnement. Nous présenterons également les différents types de sauvegarde disponibles, tels que la sauvegarde complète, la sauvegarde différentielle et la sauvegarde incrémentielle.

Enfin, nous nous concentrerons sur la réplication, ou "Backup", qui vise à maintenir la disponibilité des systèmes en créant des copies exactes des données et des configurations sur des serveurs ou des sites de secours. Nous définirons la réplication et expliquerons ses objectifs. Nous discuterons également des différents mécanismes de réplication utilisés, tels que la réplication synchrone et la réplication asynchrone.

3.1 Présentation de la supervision "Monitoring"

3.1.1 Définition

Superviser une infrastructure réseau consiste à mieux connaître son état et son niveau de performance, à garantir son bon fonctionnement et à détecter d'éventuelles pannes ou problèmes liés aux connexions et aux équipements. (12)

On surveille généralement :

— Les équipements actifs comme les routeurs , les switches, les points d'accès sans fil , etc .

— Les serveurs d'authentifications , de stockage , les annuaires ,les serveurs web , les solutions VoIP.

3.1.2 Objectif

Aujourd'hui, il est de plus en plus difficile de gérer les réseaux. En effet, le nombre d'appareils à gérer en général augmente : postes de travail, serveurs, ...
La principale préoccupation de l'administrateur est la panne. En effet, il doit pouvoir réagir au plus vite pour effectuer les réparations nécessaires.(12)

Il est nécessaire de pouvoir surveiller en permanence l'état du système informatique pour éviter des arrêts de production excessifs. C'est là qu'intervient la surveillance. Il doit permettre de prévoir les problèmes et fournir des informations sur l'état de l'équipement.

Plus le système est grand, plus la surveillance sera importante si les outils nécessaires ne sont pas disponibles.

3.1.3 principe

La plupart des logiciels de surveillance sont basés sur le protocole "SNMP" qui existe depuis de nombreuses années. La plupart de ces outils permettent de multiples fonctions dont les principales sont : (3)

— Surveiller le système d'information
— Visualiser l'architecture du système
— Analyser les problèmes
— Activer les alertes en cas de problème
— Prendre des mesures en fonction des alertes

Ensuite, cela simplifie la tâche de l'administrateur. Il lui suffit de cocher pour agir en fonction de l'alerte déclenchée. Chaque outil doit également fournir une vue globale des informations pour identifier les problèmes le plus rapidement possible.

Le protocole SNMP

3.1.4 Présentation

SNMP « Simple Network Management Protocol » : C'est le protocole de gestion des réseaux le plus utilisé . la majorité des applications de supervisons existantes sur le marché en tirent parti.

Ce protocole fonctionne suivant en mode « client / serveur », ce qui permet à un administrateur de n'obtenir les informations recueillies par les équipements réseaux que lorsqu'il en fait la demande ou lorsqu'une alerte aura été déclenchée . Il sert à gérer les équipements informatiques et réseaux, et à en diagnostiquer leur pannes . (4)

3.1.5 Les composants de SNMP

L'environnement de gestion SNMP se compose de plusieurs composants essentiels : la station de supervision (Manager), les éléments actifs du réseau, les variables MIB et les agents SNMP,voir la figure ci-dessus.(4)

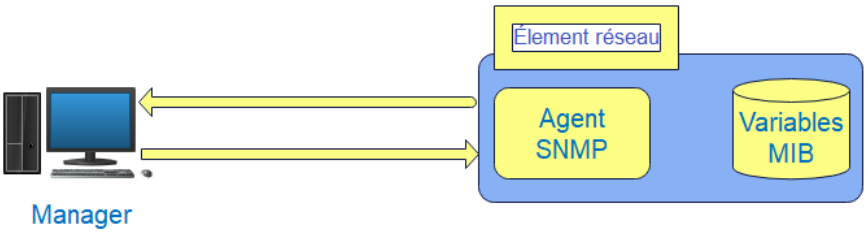


FIGURE 3.1 – L'environnement de gestion SNMP

— **La station de supervision** (Manager) : Exécute les opérations de contrôle des différents équipements informatiques à surveiller. Cette station centrale permet à l'administrateur de superviser en temps réel toute son infrastructure , diagnostiquer les problèmes et réagir pour les résoudre.
— **Les éléments réseaux à gérer ou à superviser** : Peuvent être des commutateurs , des routeurs , des points d'accès, des serveurs , des postes de travail , des imprimantes , etc. . Chaque élément dispose d'un module dit « agent » qui répond aux requêtes de la station de supervision en rapatriant l'information de gestion demandée, par exemple l'état d'un port. Les informations de gestion se trouvent dans une base de données virtuelle MIB (Management Information Base). Cette base est maintenue par l'agent, et il l'utilise pour chercher les informations de de gestion dont il a besoin.

3.1.6 fonctionnement

Les agents

Afin de permettre l'envoi des informations souhaitées par SNMP depuis une machine à superviser, il est nécessaire d'installer un agent sur celle-ci. Cet agent fonctionne en écoutant le port 161 et attend les requêtes du serveur pour y répondre. (18)

Les systèmes de management de réseaux :

L'administrateur dispose généralement d'un outil de centralisation des informations transmises par ses agents . Cet outil interroge les équipements du réseau , ce qui lui permet de gérer l'ensemble du réseau . (18)

La MIB

SNMP nécessite la définition d'un protocole d'échange et la standardisation des informations qu'il peut transporter. Ce protocole internet doit être utilisable sur des plates-formes hétérogènes, tant au niveau matériel que du système d'exploitation.(18)

C'est pourquoi on utilise la MIB (Management information Base), une base de données d'informations de gestion maintenue par l'agent, les informations sont demandées à cette base de données.

Types de messages SNMP

Les messages SNMP peuvent être des requêtes , réponses ou des alertes. Les requêtes sont envoyer par le manager vers l'agent qui réplique alors par des réponses . (4)

1- Requêtes

- **Get-Request :** Permet la rechercher d'une variable sur un agent .
- **Get-Next-Request :** Sert à obtenir la valeur de la variable suivante.
- **Set-Request :** permet de changer la valeur d'une variable sur un agent .
- **Get-Bulk :** Permet la recherche d'un ensemble de variables regroupées.

2- Réponses

- **Get-Response :** L'information a bien été transmise.
- **NoSuchObject :** Aucune variable n'a été trouvée.
- **NoAccess :** Les droits d'accès ne sont pas attribués.
- **NoWritable :** La variable ne peut être écrite.

3- Alertes :

- **trap :** L'agent SNMP envoie une alerte au Manager.

La figure suivante représente les différentes type des messages SNMP :

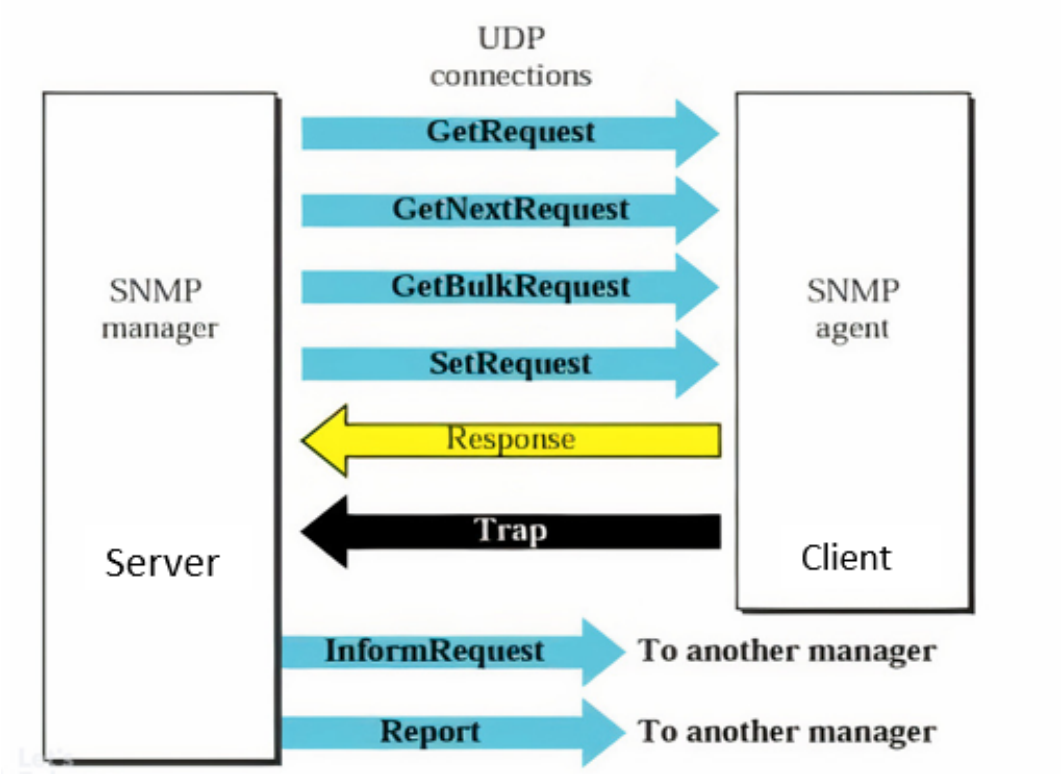


FIGURE 3.2 – type des message SNMP

Les versions de SNMP

SNMP existe au moins en trois versions : 1, 2 et 3 ; la version 1 étant la plus ancienne.

Voici les différentes versions de SNMP : (22)

* **SNMPv1**
  Ceci est la première version du protocole, définie dans le RFC (Request For Comments) 1157. On dit que la sécurité de cette version est triviale, car la seule vérification qui est faite est basée sur la chaîne de caractères " community". 28 SNMPsec (historique) : cette version ajoute de la sécurité au protocole SNMPv1. La sécurité est basée sur des groupes. Très peu ou aucun manufacturier n'a utilisé cette version qui est maintenant largement oubliée.

* **SNMPv2p**
  Beaucoup de travaux ont été exécutés pour faire une mise à jour de SNMPv1. Ces travaux ne portaient pas seulement sur la sécurité. Le résultat est une mise à jour des opérations du protocole, des nouvelles opérations, des nouveaux types de données. La sécurité est basée sur les groupes de SNMPsec.

* **SNMPv2c**
  Cette version du protocole est appelée " community string based SNMPv2 ". Ceci est une amélioration des opérations de protocole et des types d'opérations de SNMPv2p et utilise la sécurité par chaîne de caractères "community " de SNMPv1 selon le RFC – 1441

Étude des solutions de Supervision (Monitoring)

Les résultats de nos recherches préliminaires indiquent que la meilleure option pour répondre à notre besoin est une solution logicielle. Il n'existe actuellement aucun produit matériel sur le marché qui correspond à nos critères. Après avoir identifié les différentes solutions logicielles, nous avons présélectionné les suivantes :

— Icinga2 .
— SolarWinds.
— Zabbix .
— Centreon .
— Nagios .

Choix de la solution

Il existe plusieurs types d'outils de supervision, chacun ayant ses avantages et ses inconvénients. On peut les diviser en deux catégories : les solutions propriétaires coûteuses et les outils open source éprouvés. Le choix d'une solution de supervision doit prendre en compte de nombreux critères, notamment l'adaptabilité au réseau cible, qui évolue constamment avec une diversité d'équipements variables.

Ainsi, le choix des outils de supervision pour cette comparaison a été basé sur plusieurs facteurs :

— Ils sont entièrement open source.
— Ils sont encore activement pris en charge.
— Ils permettent de générer des graphiques.
— Ils fonctionnent sur différents types d'équipements tels que les commutateurs, les routeurs, les serveurs, etc.
— Ils disposent d'une interface web conviviale.

— Ils prennent en charge le SNMPv3.
— Ils avertissent les administrateurs en cas de problèmes.
Nous avons résumé notre étude comparative des différents solution dans le tableau suivante :

Solution	Icinga2	Nagios	Zabbix	Prometheus	Centreon
Flexibilité	Moyenne	Faible	Moyenne	Moyenne	Élevée
Architecture	Modulaire	Monolithique	Modulaire	Modulaire	Modulaire
Extensibilité	Bonne	Bonne	Bonne	Bonne	Excellente
SE supportés	Tous	Tous	Tous	Tous	Tous
Scalabilité	Bonne	Moyenne	Bonne	Bonne	Bonne
Convivialité	Moyenne	Moyenne	Moyenne	Moyenne	Bonne
SNMP	Oui	Oui	Oui	Non	Oui (partiel)
Avertissement	Oui	Oui	Oui	Oui	Oui

Table 3.1 – Comparaison entre différentes solutions de supervision

Après avoir comparé les différentes solutions présélectionnées et en tenant compte de nos besoins ainsi que des critères spécifiés dans notre cahier des charges, nous avons décidé d'opter pour la solution suivante : [Centreon].

Centreon se distingue comme la solution de surveillance privilégiée utilisée actuellement chez Cevital, avec l'utilisation de deux versions en alternance, la version 2.8.26 et la version 21.10.3. Bien qu'elle ne soit pas open source, Centreon est appréciée pour sa flexibilité élevée, permettant une personnalisation approfondie des configurations. Sa facilité d'extensibilité facilite l'intégration de nouvelles fonctionnalités. Centreon est compatible avec tous les systèmes d'exploitation courants, offrant ainsi une surveillance cohérente de l'ensemble de l'infrastructure de Cevital.
De plus, son interface conviviale et sa facilité de configuration en font un choix préféré. Centreon prend également en charge le protocole SNMP, essentiel pour la surveillance des équipements réseau. Globalement, Centreon se révèle être la solution de surveillance complète la mieux adaptée aux besoins de Cevital, malgré son statut non open source.

3.2 Présentation de la sauvegarde "Backup"

3.2.1 Définition

La sauvegarde réseau et système est une pratique consistant à créer des copies de sécurité des données et des configurations critiques d'un réseau informatique et d'un système d'exploitation. Elle vise à protéger les informations essentielles contre les pertes de données, les pannes matérielles, les attaques de logiciels malveillants et autres incidents. La sauvegarde réseau concerne la copie des données stockées sur les serveurs et les dispositifs de stockage en réseau, tandis que la sauvegarde système englobe la copie de l'ensemble du système d'exploitation. Ces sauvegardes permettent de restaurer rapidement le réseau et le système en cas de problème, assurant ainsi la continuité des opérations. (7)

3.2.2 Le principe

La sauvegarde peut être effectuée localement, en utilisant des supports de stockage tels que des serveurs, des disques, des bandes ou des CD-ROM, qui sont hébergés dans le système informatique (SI). Cette approche est utilisée pour permettre une restauration rapide en cas de besoin. Alternativement, la sauvegarde peut être archivée ou même externalisée.(21)(5)

3.2.3 Les types de la sauvegarde

On distingue trois types de sauvegardes :
— La sauvegarde totale (T) .
— La sauvegarde différentielle (D) .
— La sauvegarde incrémentale (I) .

1. **sauvegarde totale :**

   Une sauvegarde totale, connue également sous le nom de sauvegarde complète, consiste à effectuer une copie intégrale d'un contenu à un instant précis T , sans tenir compte de l'historique. Bien que cette méthode demande davantage de temps et d'espace, elle est considérée comme la plus fiable, car elle assure l'intégrité de toutes les données sauvegardées.

   Dans le cadre de la sauvegarde des données, il n'est pas recommandé de se limiter uniquement à la sauvegarde totale, car toutes les données ne sont généralement pas modifiées entre deux sauvegardes successives.

   Pour remédier à cela, il existe deux autres méthodes de sauvegarde qui se concentrent uniquement sur les données modifiées ou ajoutées après une sauvegarde totale : la sauvegarde incrémentale et la sauvegarde différentielle.(6)(5)(1)
2. **sauvegarde incrémentale :**

   La sauvegarde incrémentale implique de sauvegarder exclusivement les données qui ont été modifiées depuis la dernière sauvegarde, qu'il s'agisse de fichiers ajoutés, modifiés ou supprimés. Cette approche permet de réduire à la fois le temps nécessaire pour effectuer la sauvegarde et l'espace de stockage requis, car seules les modifications récentes sont prises en compte.(21)(1)
3. **sauvegarde différentielle :**

   Une sauvegarde différentielle effectue une copie des fichiers créés ou modifiés en se basant sur les différences constatées par rapport à la dernière sauvegarde complète, indépendamment des sauvegardes intermédiaires qui ont pu être réalisées.(5)(1)

3.3 Présentation de la réplication "Reckup"

3.3.1 Définition

La réplication des réseaux et systèmes est une pratique essentielle dans le domaine de l'administration et de la sécurité des réseaux et systèmes. Elle vise à créer et à maintenir des copies synchronisées des données, des applications et des configurations sur des sites distants. Cette approche permet d'assurer la disponibilité continue des services et de garantir la reprise après sinistre en cas de défaillance ou d'incident majeur.

La réplication des réseaux et systèmes repose sur plusieurs concepts et mécanismes clés. Tout d'abord, il est important de définir un point de consistance, qui correspond à un état spécifique des données et des applications à partir duquel la réplication est effectuée. Le choix du point de consistance approprié est crucial pour garantir l'intégrité des données répliquées.

3.3.2 Objectifs

- **Disponibilité :** Assurer la disponibilité continue des données ou des services, même en cas de panne d'un nœud ou d'un système.
- **Résilience :** Garantir la résilience du système en évitant les points de défaillance uniques.
- **Performance :** Améliorer les performances en répartissant la charge de travail sur plusieurs nœuds répliqués.
- **Scalabilité :** Permettre l'expansion du système en ajoutant de nouveaux nœuds répliqués pour gérer une augmentation de la charge.

3.3.3 Mécanismes de réplication

Consiste en l'ensemble de techniques utilisées pour créer et maintenir des copies synchronisées des données, des applications et des configurations sur des sites distants. deux approches courantes sont utilisées la réplication synchrone et la réplication asynchrone.

1. **Réplication synchrone :**
   Dans ce mécanisme, les mises à jour des données sont répliquées en temps réel sur les sites de réplication. Cela garantit une cohérence stricte des données, mais peut entraîner une augmentation de la latence et une dégradation des performances.
2. **Réplication asynchrone :**
   Dans ce mécanisme, les mises à jour des données sont répliquées avec un certain délai par rapport au site principal. Cela permet une meilleure évolutivité et des performances optimales, mais peut entraîner une légère incohérence des données.

Ces mécanismes de réplication peuvent être mis en œuvre à l'aide de divers outils, technologies et protocoles spécifiques. Il est important de choisir le mécanisme de réplication approprié en fonction des besoins spécifiques de l'entreprise et de ses contraintes.

Etude des solutions de Sauvegarde et réplication

Il existe une variété d'outils de sauvegarde et de réplication disponibles sur le marché, chacun offrant des fonctionnalités spécifiques pour répondre aux besoins des entreprises et des utilisateurs individuels.

Après avoir étudié différentes solutions logicielles , nous avons présélectionner certain outils de sauvegarde populaires incluent Veeam Backup & Replication , Duplicati, Commvault, Bacula .

Critères de choix de la solution

Le tableau suivant résume une comparaison des différentes solutions de sauvegarde et de réplication des données selon les principaux critères indiqués dans la première colonne.

Selon cette comparaison, Veeam Backup and Réplication est considérée comme la meilleure solution pour les grandes entreprises en raison de ses nombreux avantages. Il se distingue par sa facilité d'utilisation, son support étendu de la virtualisation, des systèmes d'exploitation et des applications, ainsi que par ses fonctionnalités avancées telles que la déduplication, la réplication de sauvegardes et une excellente intégration avec le cloud.

Veeam offre également un excellent support technique et une interface conviviale, ce qui facilite la configuration et la gestion des sauvegardes dans des environnements d'entreprise complexes.

Fonctionnalité	Veeam Backup & Replication	Duplicati	Commvault	Bacula
Facilité d'utilisation	Très élevée	Élevée	Moyenne à élevée	Moyenne
Support de la virtualisation	Oui	Non	Oui	Oui
Support des systèmes d'exploitation	Large	Limité	Large	Large
Fonctions de déduplication	Oui	Oui	Oui	Oui
Réplication de sauvegardes	Oui	Non	Oui	Oui
Intégration du cloud	Très bonne	Bonne	Bonne	Moyenne
Prise en charge des applications	Large	Limitée	Large	Large
Interface de gestion	Conviviale	Simple	Complexe	Complexe
Support technique	Bon	Variable	Bon	Variable
Coût	Élevé	Gratuit	Élevé	Variable

Table 3.2 – Comparaison entre différentes solutions de Backup et Réplication

Malgré un coût potentiellement plus élevé par rapport à d'autres solutions, Veeam offre une valeur significative grâce à sa performance, sa fiabilité et ses fonctionnalités étendues. Pour les grandes entreprises qui ont besoin d'une solution de sauvegarde robuste, conviviale et intégrée, Veeam Backup and Réplication est le choix idéal.

Conclusion

Lors de cette présentation, nous avons offert une vue d'ensemble complète de la supervision, de la sauvegarde et de la réplication, en mettant en évidence leur importance dans la gestion des réseaux et des systèmes informatiques. Nous avons fourni aux lecteurs une compréhension approfondie des concepts fondamentaux, des principes de fonctionnement et des objectifs associés à ces domaines essentiels de la gestion des technologies de l'information.

Après avoir réalisé une analyse comparative des solutions disponibles, nous avons décidé d'adopter la solution Centreon en raison de sa flexibilité, de sa compatibilité avec les systèmes d'exploitation courants et de son interface conviviale. En ce qui concerne les exigences de sauvegarde et de réplication du réseau et des systèmes, nous avons opté pour la solution Veeam Backup & Replication.

En conclusion, la solution Centreon a été sélectionnée pour la supervision des réseaux et des systèmes, tandis que la solution Veeam Backup & Replication a été choisie pour garantir la sauvegarde et la réplication. Ces choix sont basés sur une analyse approfondie de l'existant et visent à améliorer la gestion et la fiabilité du réseau de CEVITAL.

Chapitre 4

Réalisation et test

Introduction

Dans ce chapitre nous concentrons sur la phase de mise en œuvre de ce projet, qui constitue le corps principal de ce mémoire. Nous présenterons en détail les prérequis et les étapes de configuration nécessaires à l'installation de différents logiciels et systèmes, accompagnés de captures d'écran illustratives.

4.1 Environnement de travail

4.1.1 Installation de GNS3 sous windows :

Définition

GNS3 (Graphical Network Simulator) est un logiciel libre permettant l'émulation ou la simulation de réseaux informatiques.
La figure ci-dessus représente le logo de GNS3.

FIGURE 4.1 – GNS3

Installation de GNS3 sous Windows

Afin d'installer GNS3, il est nécessaire de procéder en suivant ces étapes : télécharger d'abord le fichier exécutable, puis le lancer et suivre les instructions d'installation jusqu'à leur terme. Enfin, il suffit de cliquer sur le bouton "Finish" pour finaliser le processus.

La capture d'écran ci-dessous illustre l'interface de GNS3.

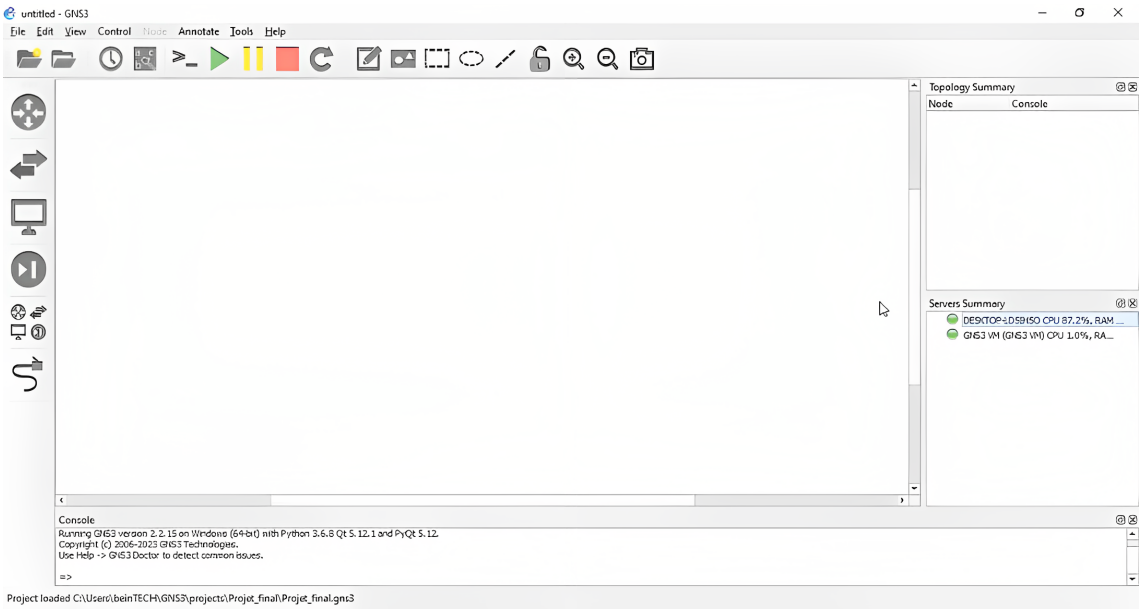


FIGURE 4.2 – Interface d'accueil GNS3

4.1.2 Installation de VMware Workstation version 17 pro

Définition

Il s'agit d'un logiciel de machine virtuelle de VMWare Inc. Il permet plusieurs copies du même système d'exploitation ou il peut y avoir plusieurs systèmes d'exploitation différents qui peuvent s'exécuter simultanément sur la même machine x86. Il prend en charge plusieurs systèmes d'exploitation exécutés sur un PC Windows ou Linux. Il dispose également d'outils de déploiement comme VMWare ACE. Le bureau d'un utilisateur peut être stocké sur une clé USB pour le transport. Il s'agit du processus de création d'un logiciel ou d'une représentation virtuelle qui inclut des serveurs, du stockage et différents réseaux. Il agit efficacement comme une solution pour réduire les dépenses informatiques et augmenter l'efficacité et l'agilité, La figure ci-dessus représente le logo de.(**?**)

FIGURE 4.3 – VMware Workstation

Installation de la VMware Workstation 17pro

Afin d'installer VMware Workstation 17 pro , il est nécessaire de procéder en suivant ces étapes : télécharger d'abord le fichier exécutable, puis le lancer et suivre les étapes de la figure ci-dessous :

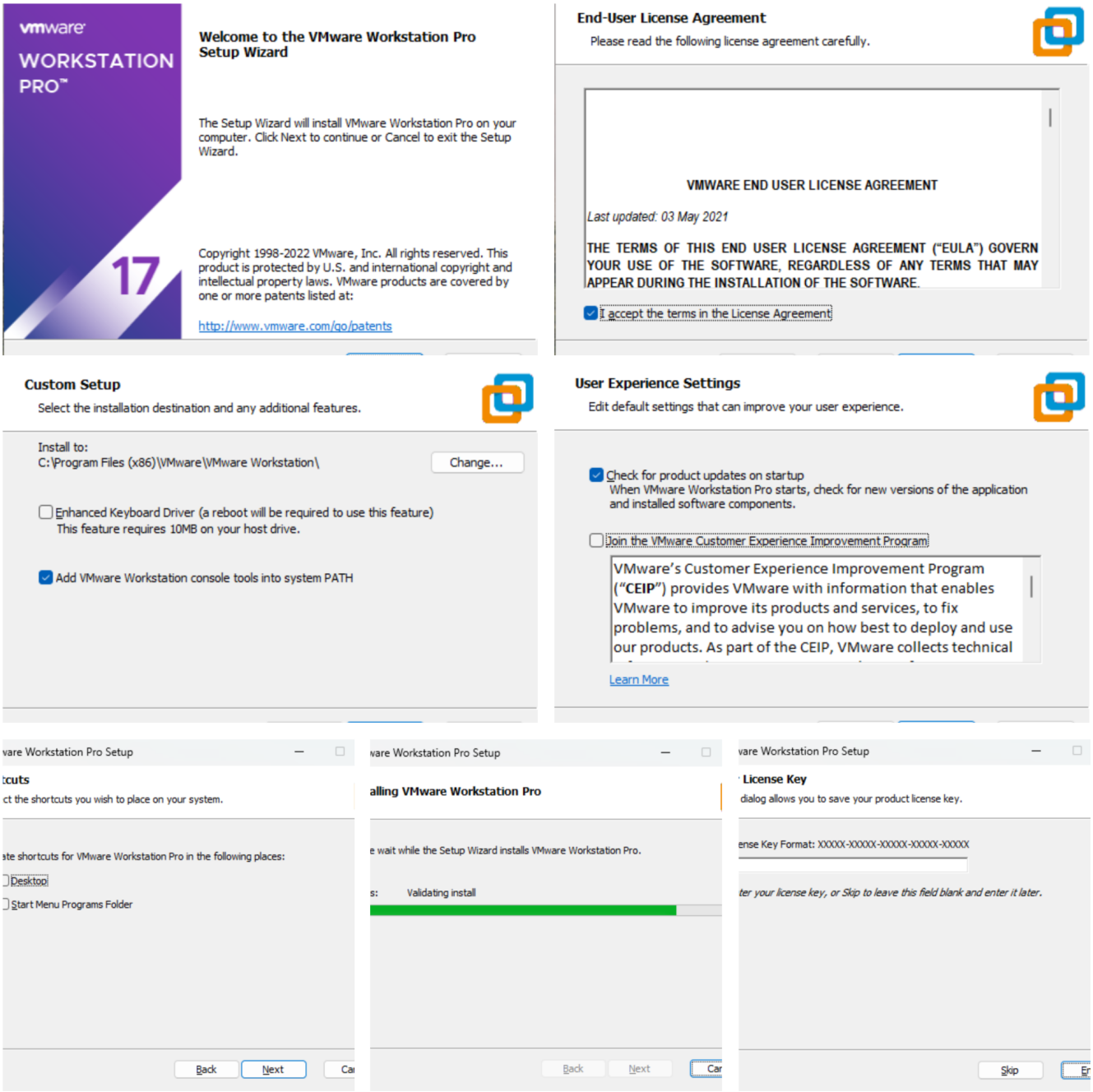


FIGURE 4.4 – Installation de VMware workstation

Après avoir installé VMware, vous serez accueilli par une page d'accueil. Cette page d'accueil peut fournir diverses options et fonctionnalités pour vous permettre de gérer vos machines virtuelles.

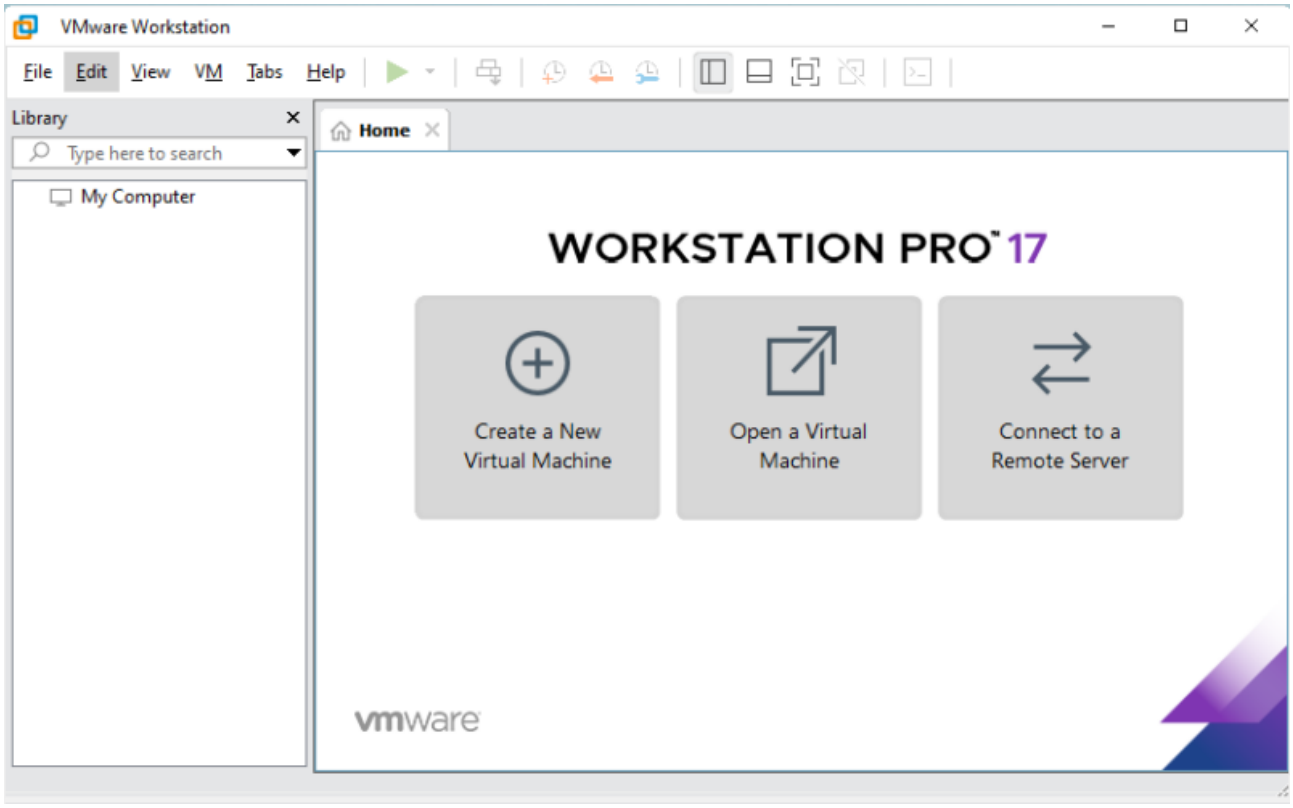


FIGURE 4.5 – Page d'accueil de VMware Workstation

4.1.3 Installation des serveurs

Installation du Windows server 2022

Dans cette partie nous allons voir les différentes étapes d'installations du Windows Server 2022,voir la figure ci-dessus.

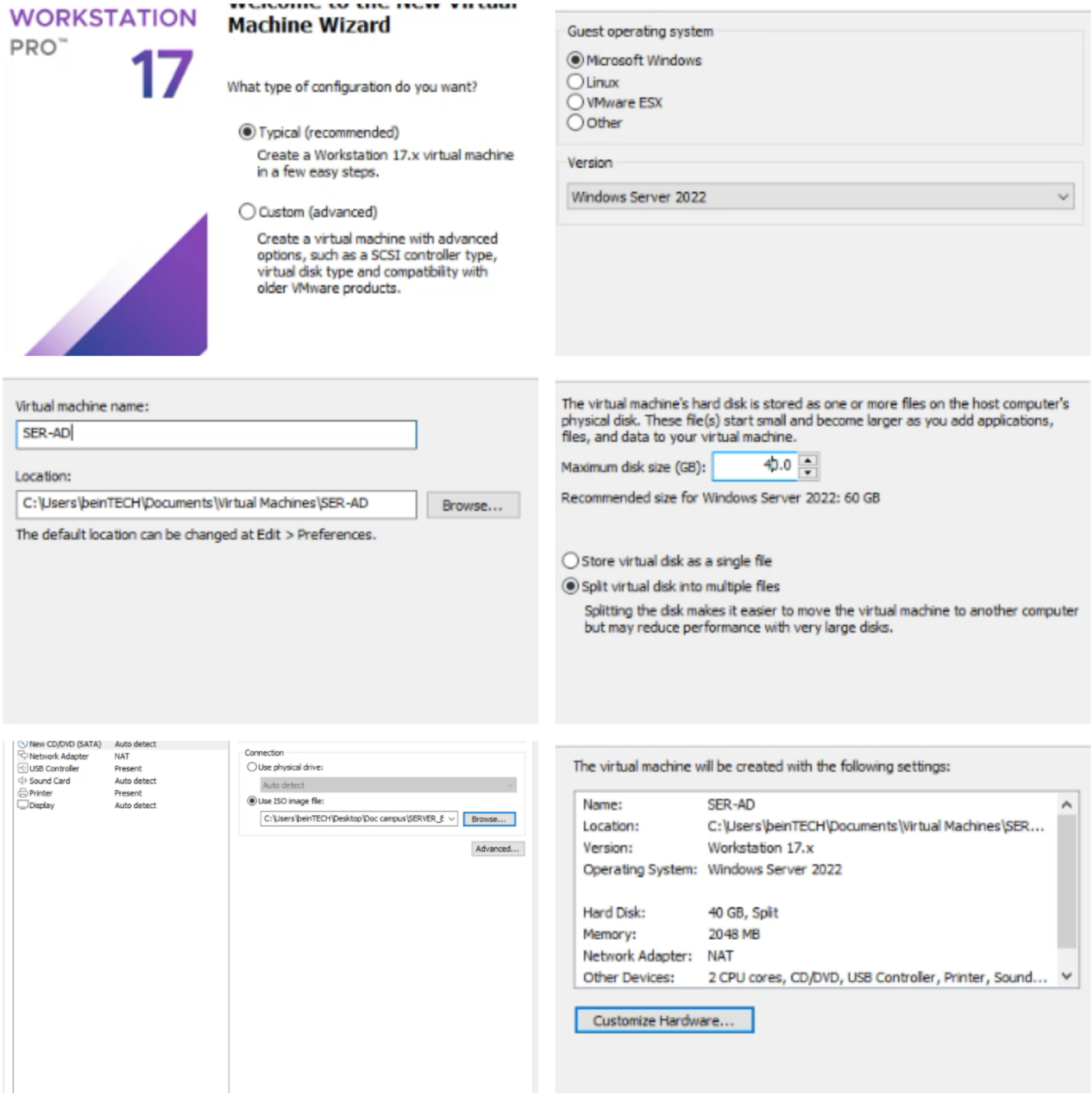


FIGURE 4.6 – Les étapes installation Windows server 2022

Installation du Linux server " Debian 11.X 64 bit"

Dans cette partie nous allons voir les différentes étapes d'installations du Linux server " Debian 11.X64bit",voir la figure ci-dessus.

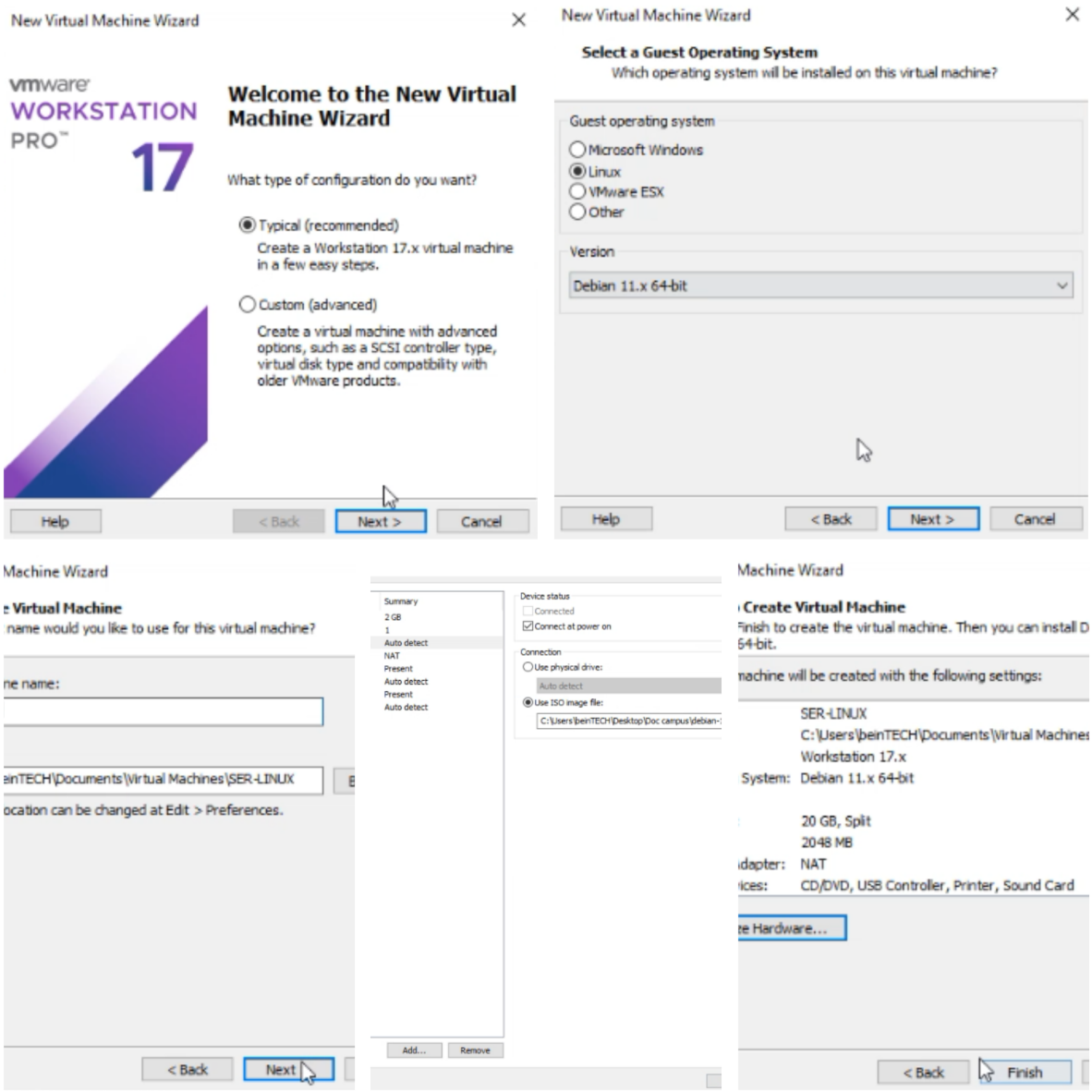


FIGURE 4.7 – Les étapes d'installation Linux server " Debian 11.X 64 bit"

Installation Client Windows 10 " Manager "

la figure ci-dessous montre les étapes à suivre dans l'ordre pour Installer Windows 10

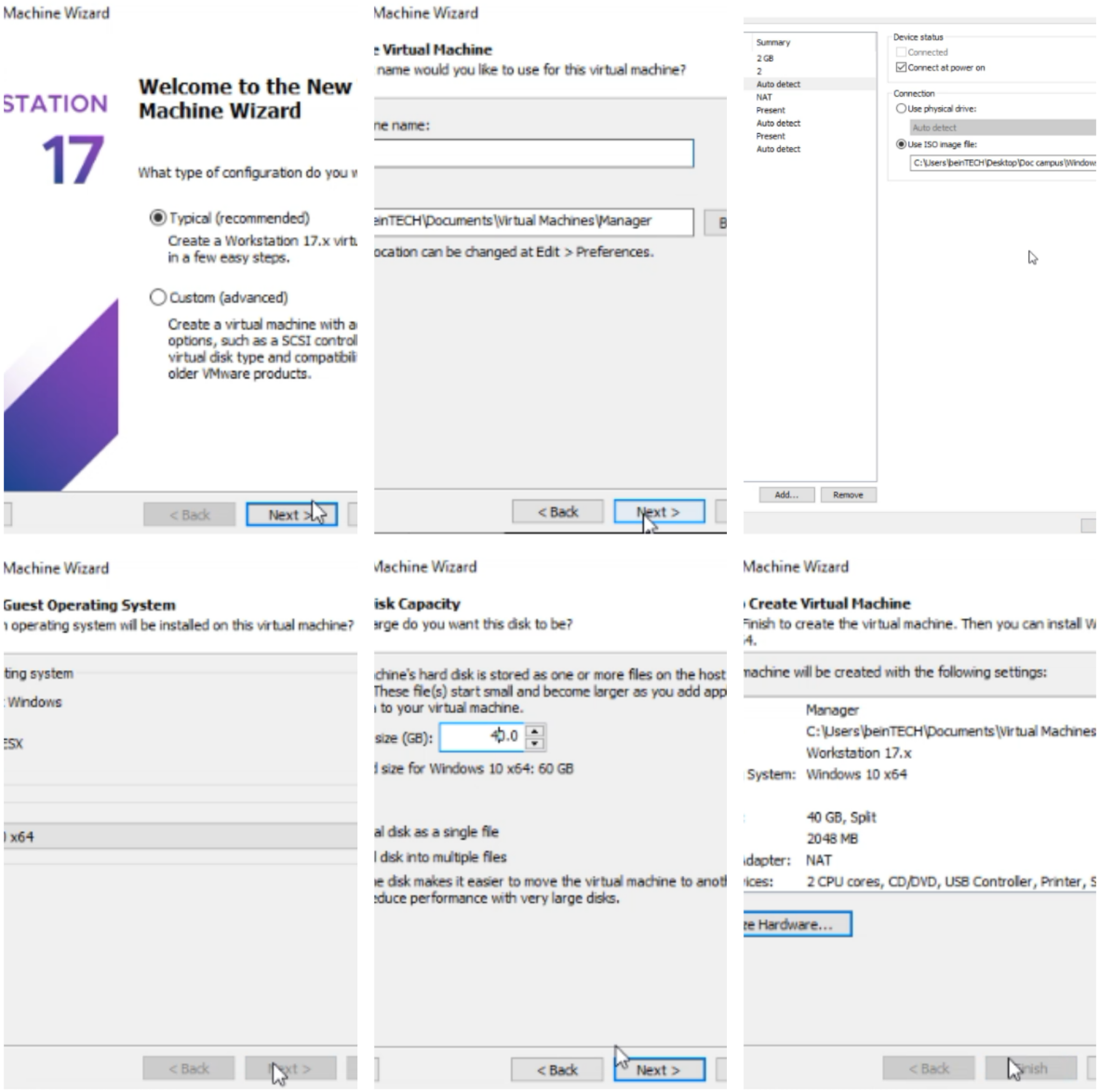


FIGURE 4.8 – Les étapes d'installation Windows 10

4.2 Architecture proposée

l'architecture proposée à l'entreprise.

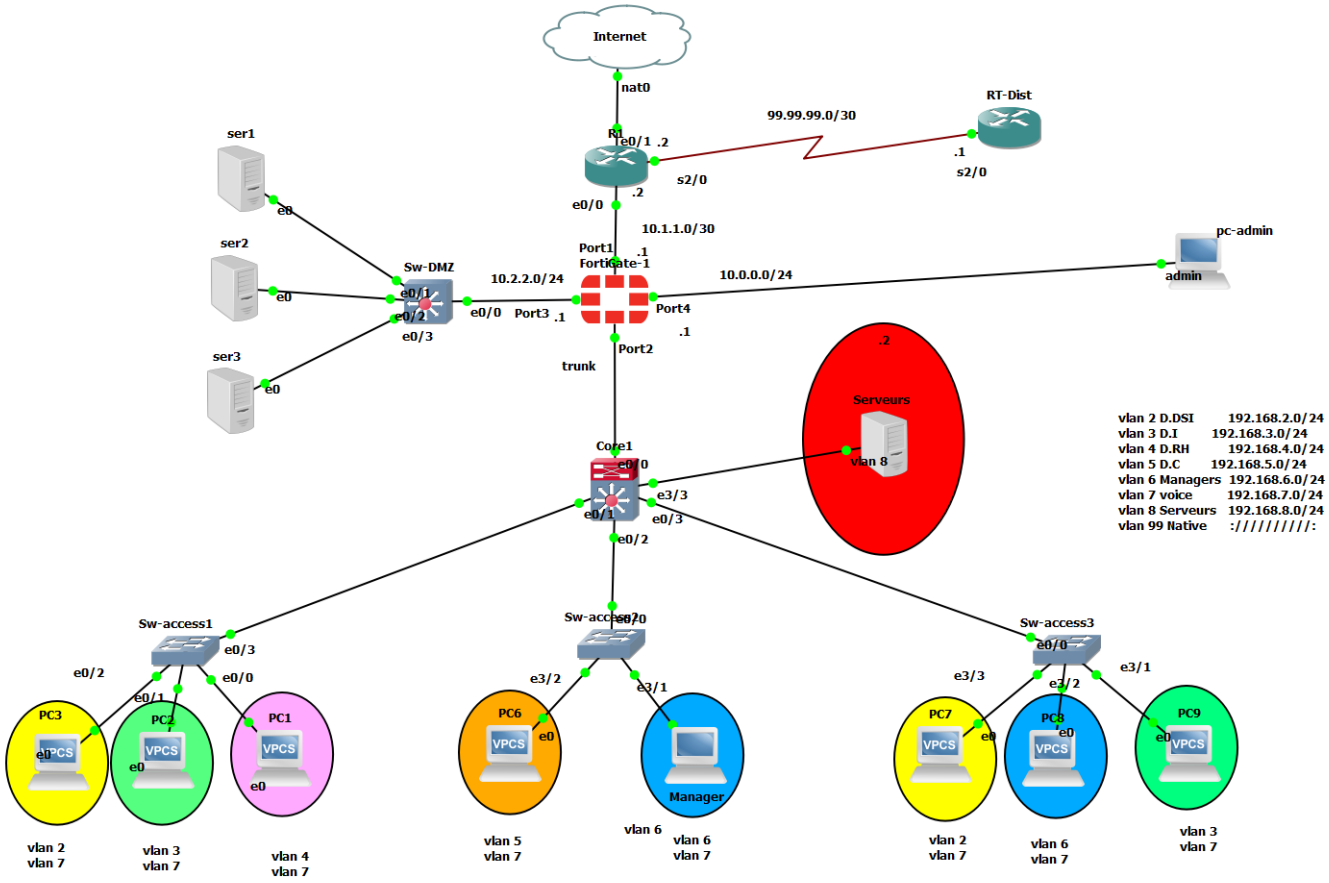


FIGURE 4.9 – Architecture proposée

4.3 Configuration des équipements

Dans cette partie,nous allons présenter la configuration en générale des équipements qui vont nous permettre de mettre en place la nouvelle architecture proposée.

4.3.1 Le plan d'adressage des VLANs

Le tableau ci-dessus représente le plan d'adressage des VLANs

Nom de vlans	Id vlan	Adresse sous réseau	Passerelle de sous réseau
D.DSI	2	192.168.2.0 / 24	192.168.2.1
RI	3	192.168.3.0 / 24	192.168.3.1
D.RH	4	192.168.4.0 /24	192.168.4.1
D.RC	5	192.168.5.0 /24	192.168.5.1
Manager	6	192.168.6.0 /24	192.168.6.1
Voice	7	192.168.7.0 /24	192.168.7.1
Serveur	8	192.168.8.0 /24	192.168.8.1
Native	99	/	/

Table 4.1 – Plan d'adressage des VLANs

4.3.2 Le plan d'adressage des équipements

Le tableau ci-dessus représente le plan d'adressage des équipements.

Équipements	Interfaces	Adressage
R1	e0/1 s2/0 e0/0	Connexion internet obtenue par dhcp 99.99.99.2 10.1.1.2
RT-Dist	S2/0	99.99.99.1
FortiGate-1	Port1 Port2 Port3 Port4	10.1.1.1 Trunk 10.2.2.1 10.0.0.1
Core1	vlan 8	192.168.8.0
Sw-access1	Vlan 2 Vlan 3 Vlan 4 Vlan 7	192.168.2.0 192.168.3.0 192.168.4.0 192.168.7.0
Sw-access2	Vlan 5 Vlan 6 Vlan 7	192.168.5.0 192.168.6.0 192.168.7.0

Table 4.2 – Plan d'adressage des équipements

4.4 Méthodologie

Le schéma de la figure 4.10 montre les étapes suivies pour la configuration de la topologie.

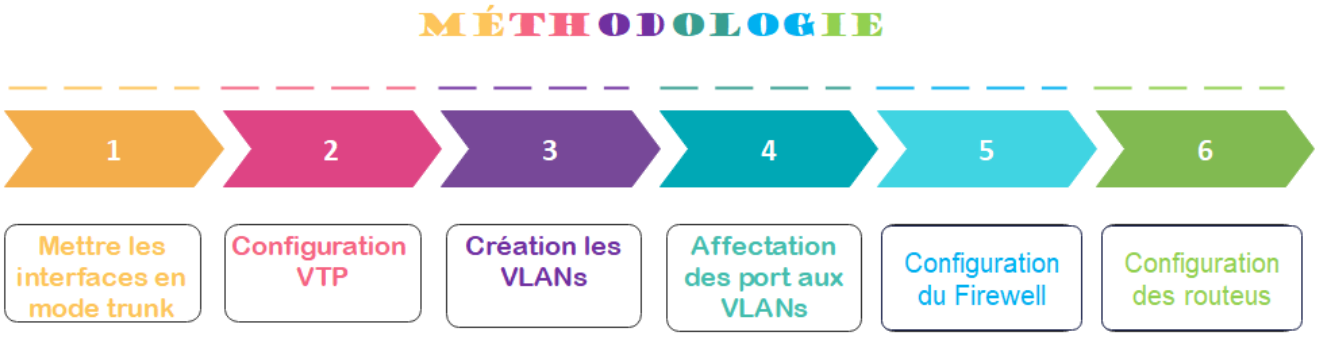


FIGURE 4.10 – Les étapes de la méthodologie

4.4.1 Mettre les interfaces en mode Trunk

1- Mettre le switch Core en mode Trunk :

Premièrement, nous avons affiché les voisins du switch Core.

```
Core1#show  cdp neighbors
Capability Codes: R - Router, T - Trans Bridge, B - Source Route Bridge
                  S - Switch, H - Host, I - IGMP, r - Repeater, P - Phone,
                  D - Remote, C - CVTA, M - Two-port Mac Relay

Device ID        Local Intrfce     Holdtme    Capability  Platform  Port ID
SW-Dist1         Eth 3/2           133             R S I  Linux Uni Eth 3/2

Total cdp entries displayed : 1
```

FIGURE 4.11 – Afficher les voisins du switch core

Deuxièmement, nous avons mis le switch Core en mode trunk.

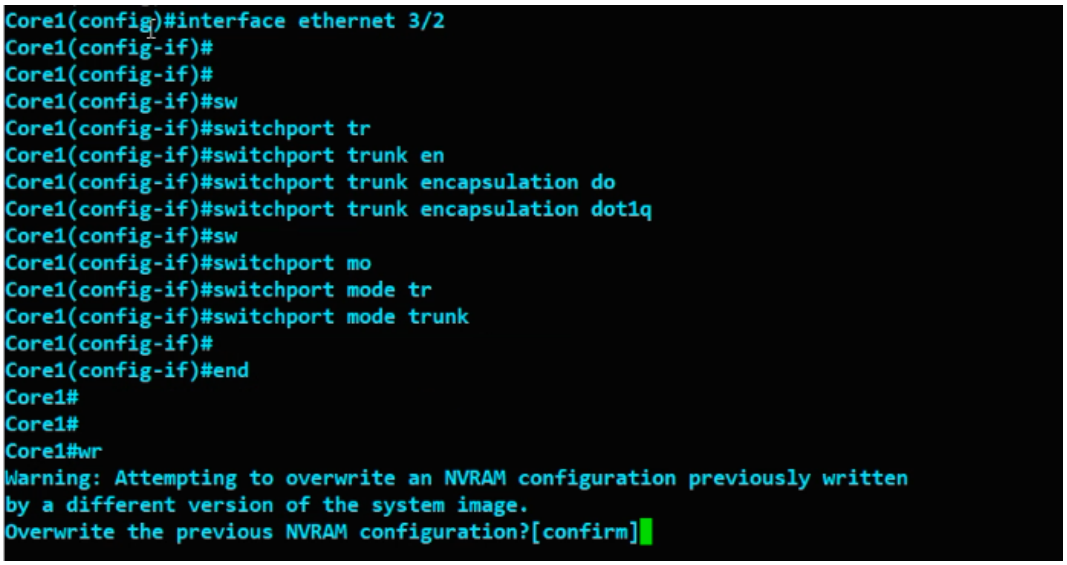


FIGURE 4.12 – Mettre le switch Core en mode Trunk

2- Mettre les switches d'accès en mode Trunk :

La figure ci-dessus montre les étapes nécessaires pour mettre le switch d'accès 1 en mode Trunk.

Nous allons effectuer les mêmes étapes avec les deux autres switches d'accès.

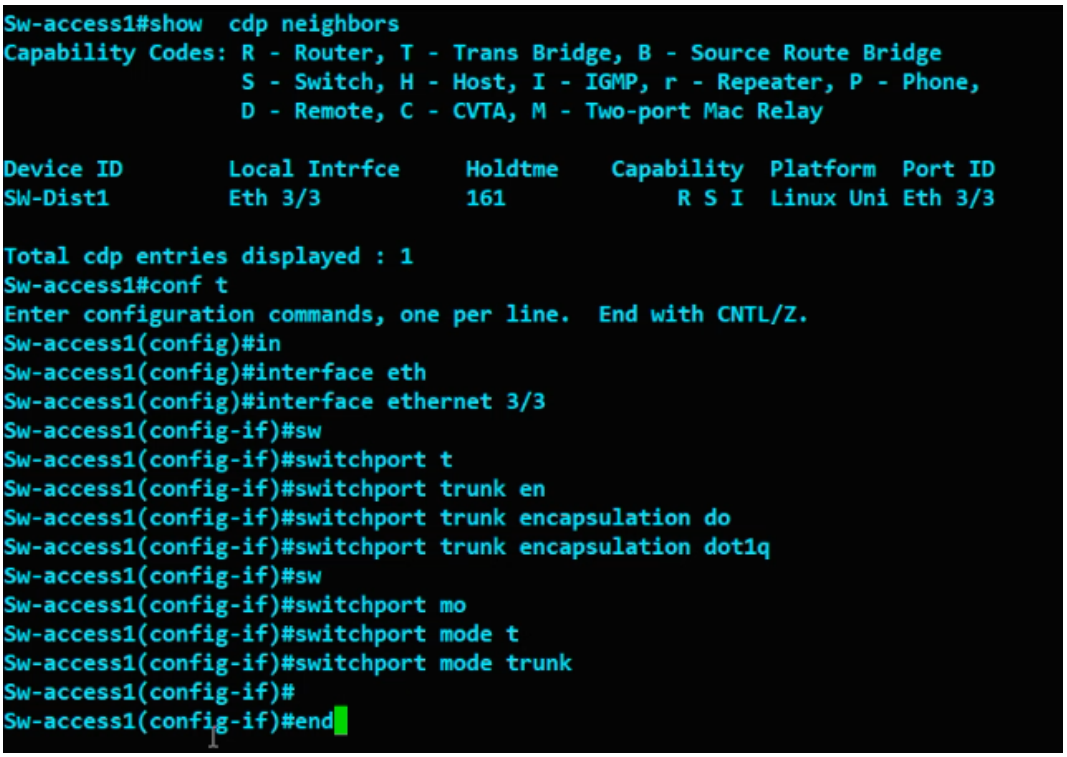


FIGURE 4.13 – Mettre le switch d'accès 1 en mode Trunk

Afin de vérifier cette configuration, on affiche l'état des interfaces avec la commande :**"show interfaces trunk"** ou bien la commande **"show interfaces status"**

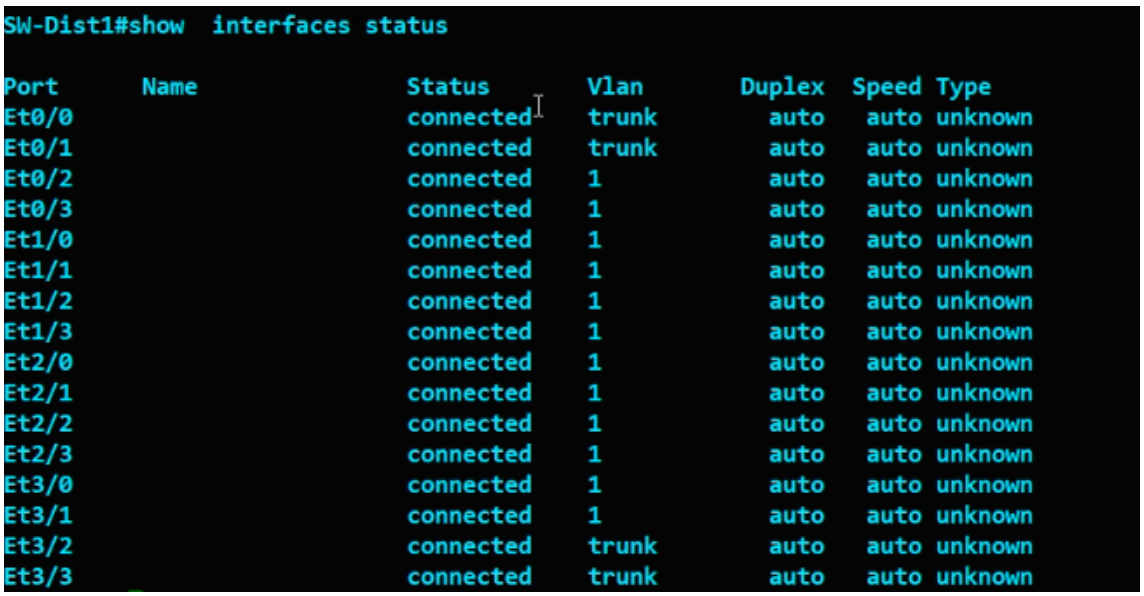


FIGURE 4.14 – afficher l'état des interfaces

4.4.2 Configuration VTP

Afin de profiter des services VTP, nous avons configuré le switch Core en mode serveur et le reste des switches d'accès en mode client. Cela a permis la propagation des VLANs du Core1 vers les autres switches d'accès.

Configuration VTP du switch Core

En configurant le switch Core en tant que serveur VTP, les VLANs pourront être propagés vers les switches d'accès.

Nous avons utilisé la commande **"vtp pruning"** sur le switch Core pour activer la fonction de pruning VTP. Cela nous a permis de restreindre la propagation des informations de VLAN uniquement aux liens trunks nécessaires, réduisant ainsi le trafic inutile sur le réseau. L'activation du pruning VTP sur le switch Core a contribué à optimiser l'utilisation de la bande passante en éliminant les VLANs non nécessaires sur les trunks et à améliorer les performances du réseau.

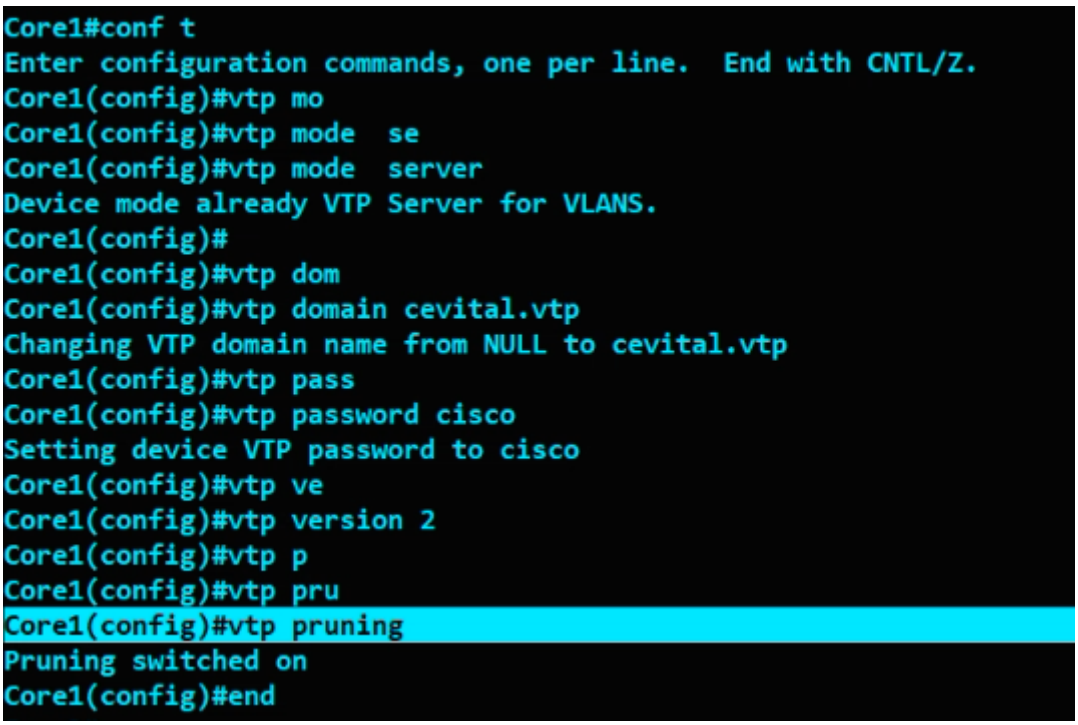


FIGURE 4.15 – Configuration VTP du switch Core

Configuration VTP des switches d'accès

En configurant les switches d'accès en tant que clients VTP, ils pourront recevoir les mises à jour des VLANs provenant du switch Core.

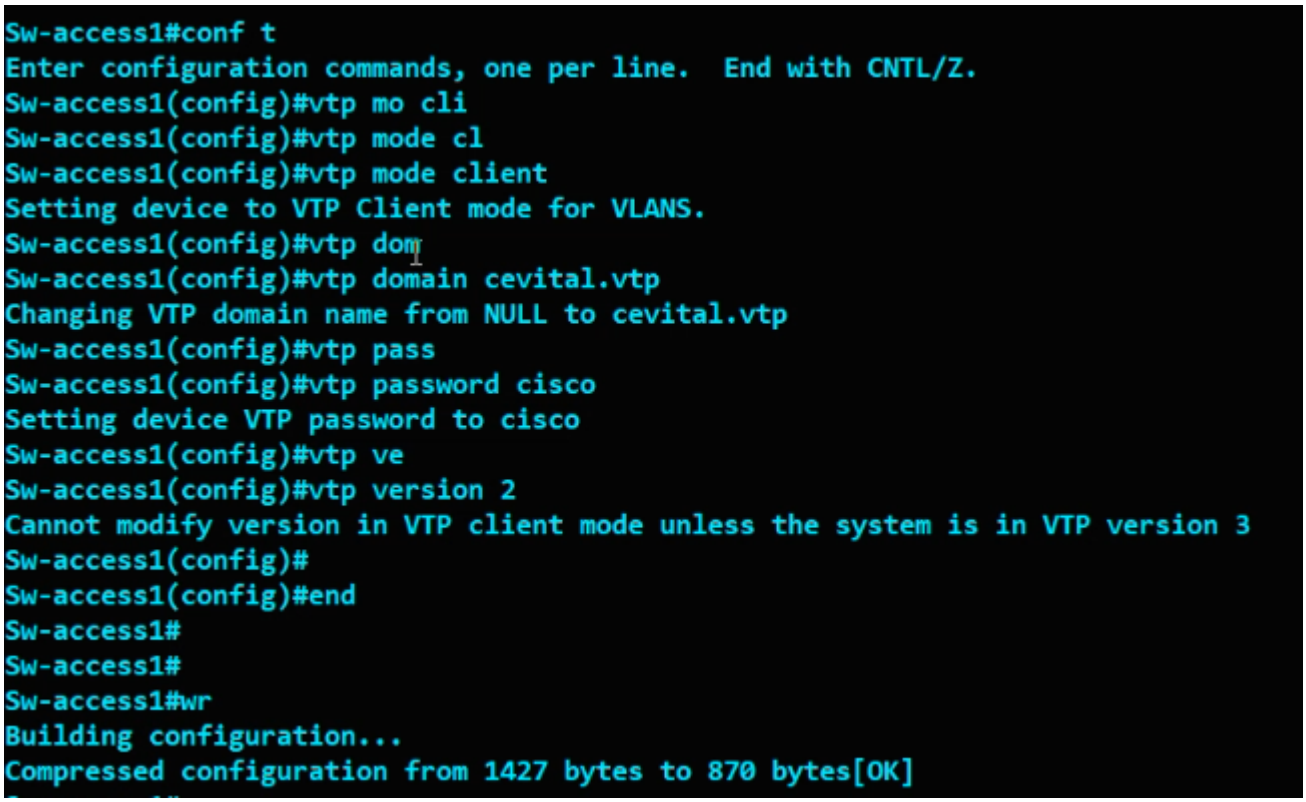


FIGURE 4.16 – Configuration VTP de switch d'accès 1

Afin de vérifier la configuration et le fonctionnement du protocole VTP , nous allons utiliser la commande : **"show vtp status"**

```
Core1#show  vtp st
Core1#show  vtp status
VTP Version capable             : 1 to 3
VTP version running             : 2
VTP Domain Name                 : cevital.vtp
VTP Pruning Mode                : Enabled
VTP Traps Generation            : Disabled
Device ID                       : aabb.cc80.0100
Configuration last modified by 0.0.0.0 at 4-6-23 11:18:05
Local updater ID is 0.0.0.0 (no valid interface found)

Feature VLAN:
--------------
VTP Operating Mode              : Server
Maximum VLANs supported locally : 1005
Number of existing VLANs        : 5
Configuration Revision          : 2
MD5 digest                      : 0xE1 0x9C 0xAD 0xD9 0x2E 0x5F 0x49 0x68
                                  0x6E 0x68 0xE3 0xBD 0xF9 0xED 0x69 0x7A
Core1#
```

FIGURE 4.17 – vérifier la configuration et le fonctionnement du protocole VTP

4.4.3 Création des VLANs

Pour créer les VLANs sur le switch Core 1 en utilisant la commande "vlan" dans le mode de configuration, puis leur donner des noms à l'aide de la commande "name" dans le même mode comme suit :

```
conf t
configuration commands, one per line.  End with CNTL/Z.
config)#
config)#vlan
config)#vlan 2
config-vlan)#name D.DSI
```

FIGURE 4.18 – Création des VLANs

Pour vérifier la création des VLANs sur le switch Core 1, nous allons utiliser la commande **"show vlan brief"**.

```
Core1#show vlan brief

VLAN Name                             Status    Ports
---- -------------------------------- --------- -------------------------------
1    default                          active    Et1/0, Et1/1, Et1/2, Et1/3
                                                Et2/0, Et2/1, Et2/2, Et2/3
                                                Et3/0, Et3/1
2    D.DSI                            active
3    RI                               active
4    D.RH                             active
5    DC                               active
6    Managers                         active
7    voice                            active
8    serveurs                         active    Et3/3
99   native                           active
1002 fddi-default                     act/unsup
1003 trcrf-default                    act/unsup
1004 fddinet-default                  act/unsup
1005 trbrf-default                    act/unsup
Core1#
```

FIGURE 4.19 – vérifier la création des VLANs

Sécurisation du vlan natif

Sécuriser le VLAN natif est important pour prévenir les attaques, isoler le trafic, contrôler l'accès et éviter les erreurs de configuration.

Nous allons effectuer les mêmes étapes avec les switches d'accès.

```
Core1#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Core1(config)#
Core1(config)#in
Core1(config)#interface  eth
Core1(config)#interface  ethernet 3/2
Core1(config-if)#sw
Core1(config-if)#switchport tr
Core1(config-if)#switchport trunk na
Core1(config-if)#switchport trunk native v
Core1(config-if)#switchport trunk native vlan 99
Core1(config-if)#sw
Core1(config-if)#switchport t
Core1(config-if)#switchport trunk all
Core1(config-if)#switchport trunk allowed vla
Core1(config-if)#switchport trunk allowed vlan 2-8,99
Core1(config-if)#
Core1(config-if)#end
```

FIGURE 4.20 – Sécurisation du vlan native

4.4.4 Affectation des ports aux VLANs

Dans cette étape, nous allons assigner des ports aux VLANs au niveau des switches d'accès avec les commandes montrées dans la figure ci-dessous :

```
Sw-access1(config)#interface eth
Sw-access1(config)#interface ethernet 0/0
Sw-access1(config-if)#sw
Sw-access1(config-if)#switchport mo
Sw-access1(config-if)#switchport mode  acc
Sw-access1(config-if)#switchport mode  access
Sw-access1(config-if)#
Sw-access1(config-if)#sw
Sw-access1(config-if)#switchport  acc
Sw-access1(config-if)#switchport  access vl
Sw-access1(config-if)#switchport  access vlan 4
Sw-access1(config-if)#sw
Sw-access1(config-if)#switchport voi
Sw-access1(config-if)#switchport voice vl
Sw-access1(config-if)#switchport voice vlan 7
Sw-access1(config-if)#
Sw-access1(config-if)#end
```

FIGURE 4.21 – Affectation des ports aux vLANs

On vérifie si les ports sont bien affectées avec la commande "**show vlan brief**" comme montré dans la figure ci-dessous :

```
Core1#show vlan brief

VLAN Name                             Status    Ports
---- -------------------------------- --------- -------------------------------
1    default                          active    Et1/0, Et1/1, Et1/2, Et1/3
                                                Et2/0, Et2/1, Et2/2, Et2/3
                                                Et3/0, Et3/1
2    D.DSI                            active
3    RI                               active
4    D.RH                             active
5    DC                               active
6    Managers                         active
7    voice                            active
8    serveurs                         active    Et3/3
99   native                           active
1002 fddi-default                     act/unsup
1003 trcrf-default                    act/unsup
1004 fddinet-default                  act/unsup
1005 trbrf-default                    act/unsup
Core1#
```

FIGURE 4.22 – vérifier si les ports sont bien affectées

4.4.5 Configuration du Firewell

Création d'un utilisateur "admin"

Premièrement, nous allons créer un utilisateur "admin" avec un mot de passe "admin".

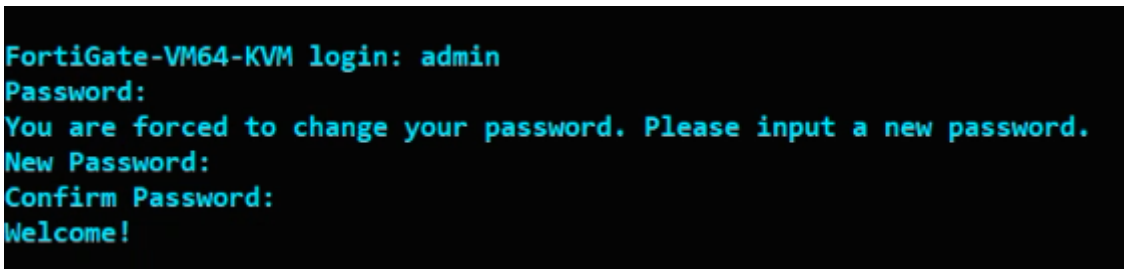


FIGURE 4.23 – Création du utilisateur "admin"

Configuration du port 4

Deuxièmement, nous allons configurer le port 4 .

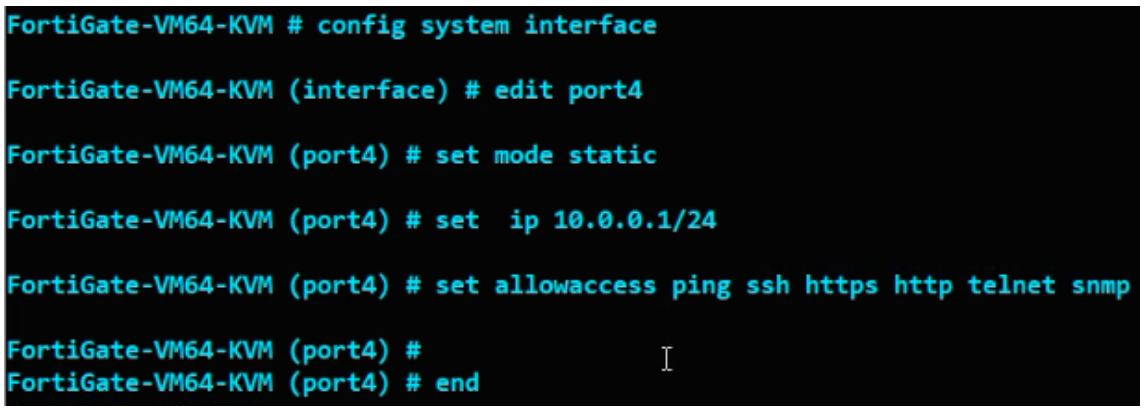


FIGURE 4.24 – Configuration du port 4

Après cela, nous allons accéder au pare-feu (firewall) en utilisant le compte administrateur (admin).

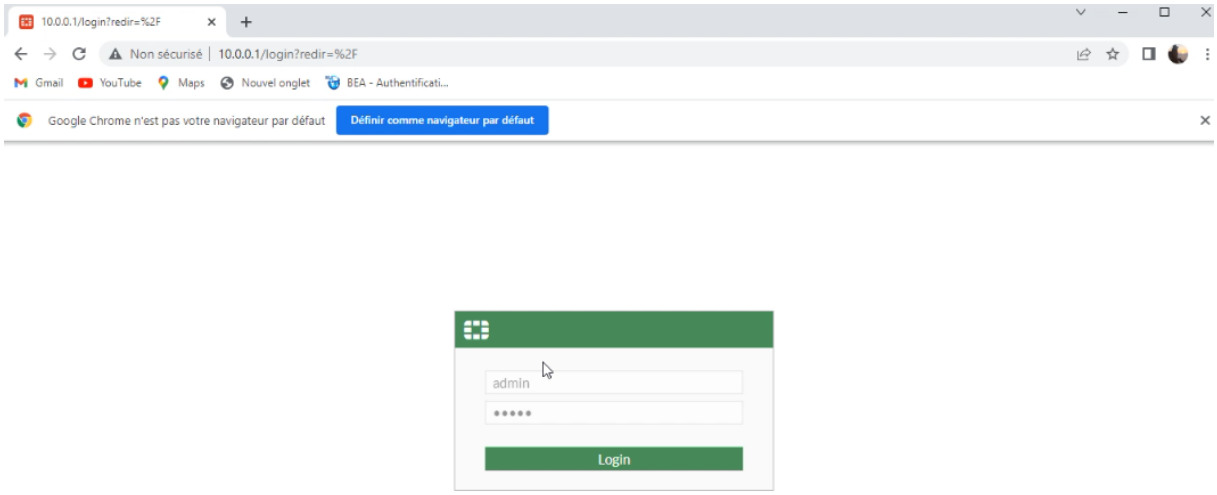


FIGURE 4.25 – Accéder au pare-feu

Modifier le nom du pare-feu

Ensuite, nous allons modifier le nom du pare-feu (firewall) pour le changer en "FortiGate-1".

```
FortiGate-VM64-KVM # config system global

FortiGate-VM64-KVM (global) # set hostname FortiGate-1
```

FIGURE 4.26 – Renommer le pare-feu

Voici l'interface d'accueil du pare-feu (firewall)

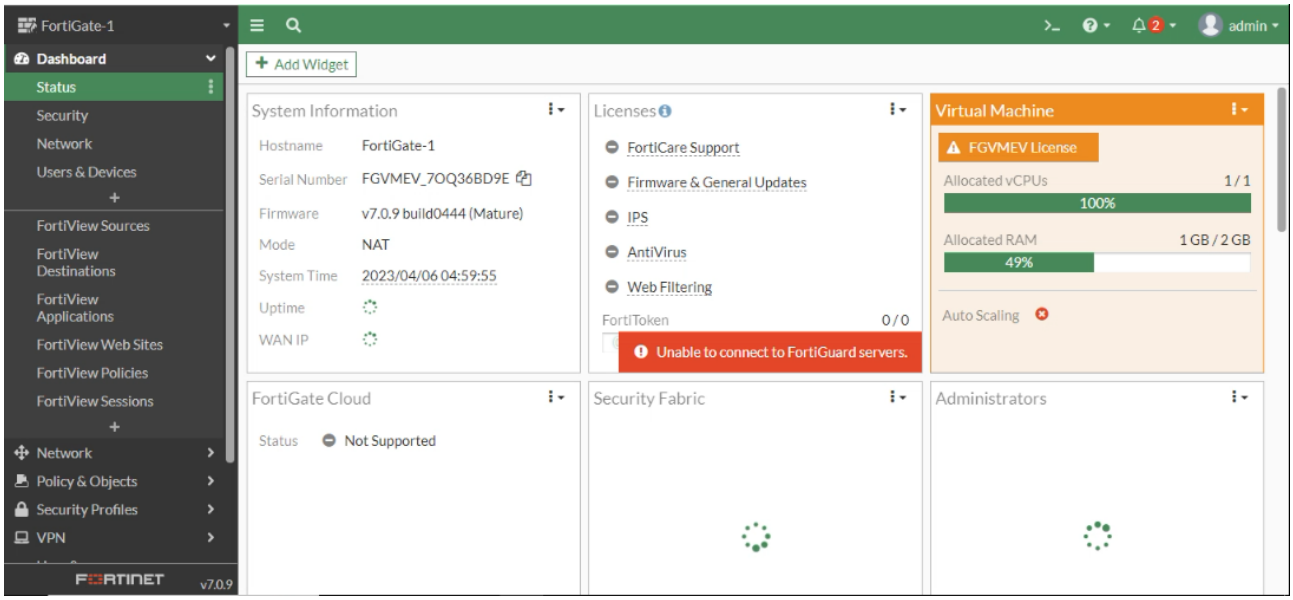


FIGURE 4.27 – Interface d'accueil du pare-feu

Configuration des portes 1, 2 et 3

La figure ci-dessus présente les portes une fois configurées.

Name	Type	Members	IP/Netmask	Administrative Access
802.3ad Aggregate 1				
fortilink	802.3ad Aggregate		Dedicated to FortiSwitch	PING Security Fabric Connection
Physical Interface 17				
INTER-VLAN (port2)	Physical Interface		0.0.0.0/0.0.0.0	PING
Internet (port1)	Physical Interface		10.1.1.1/255.255.255.252	PING HTTPS SSH HTTP FMG-Access
LINK-DMZ (port3)	Physical Interface		10.2.2.1/255.255.255.0	PING

FIGURE 4.28 – Configuration des portes 1, 2 et 3

Création du routage inter-vLANs sur le port 2

La figure ci-dessus présente les VLANs après leur création.

Name	Type	Members	IP/Netmask	Administrative Access	DHCP Clients	DHCP Ranges	Ref.
INTER-VLAN (port2)	Physical Interface		0.0.0.0/0.0.0.0	PING			7
D.DSI (vlan 2)	VLAN		192.168.2.1/255.255.255.0	PING			2
D.RC (vlan 5)	VLAN		192.168.5.1/255.255.255.0	PING		192.168.5.10-192.168.5.100	3
D.RH (vlan 4)	VLAN		192.168.4.1/255.255.255.0	PING			2
Managers (vlan 6)	VLAN		192.168.6.1/255.255.255.0	PING HTTPS HTTP		192.168.6.10-192.168.6.254	3
RI (vlan 3)	VLAN		192.168.3.1/255.255.255.0	PING			2
Serveurs (vlan 8)	VLAN		192.168.8.1/255.255.255.0	PING SNMP			2
Voice (vlan 7)	VLAN		192.168.7.1/255.255.255.0	PING			2

FIGURE 4.29 – Les VLANs

Autorisation d'accès à Internet pour le port 1.

Afin de permettre l'accès à Internet via le port 1 de notre pare-feu, il est nécessaire de suivre les étapes décrites dans la figure ci-dessus pour créer une nouvelle règle de filtrage. Cette règle devra autoriser spécifiquement le trafic sortant provenant du port 1 et dirigé vers Internet.

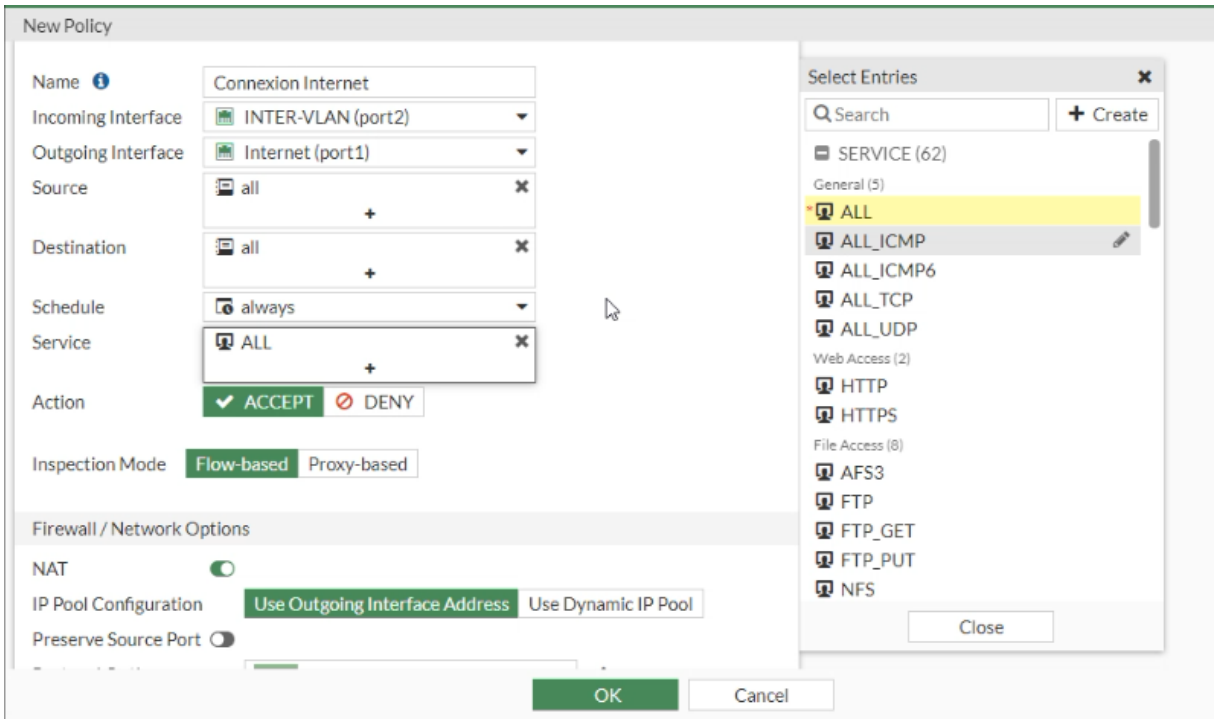


FIGURE 4.30 – Création du nouvelle règle de filtrage

4.4.6 Configuration des routeurs

Configuration du routeur R1

Premièrement, nous allons configurer les interfaces Ethernet 0/0 et 0/1.

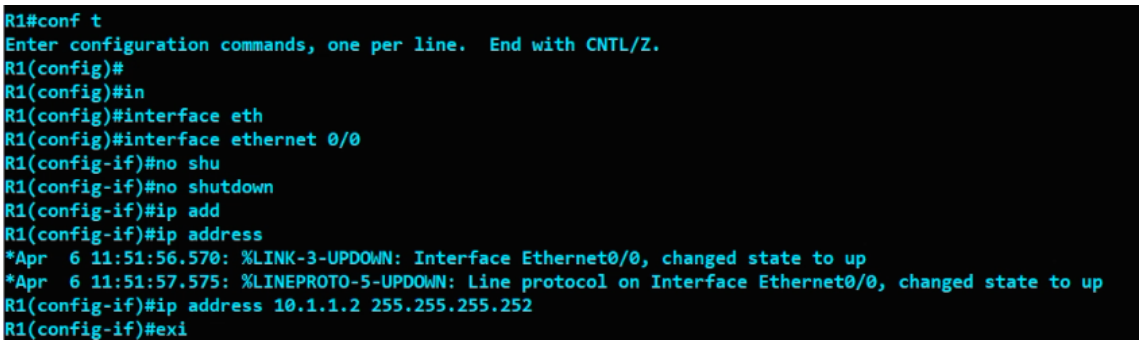


FIGURE 4.31 – Configuration du l'interface ethernet 0/0

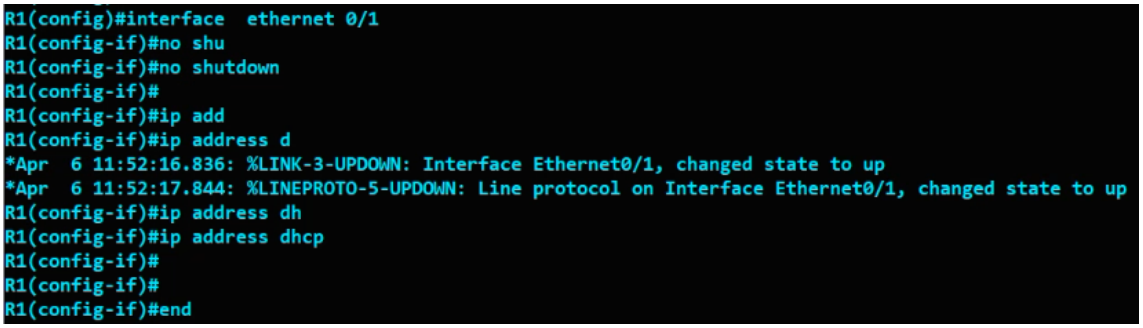


FIGURE 4.32 – Configuration du l'interface ethernet 0/1

Deuxièmement, nous allons renommer R1 en tant que FAI.

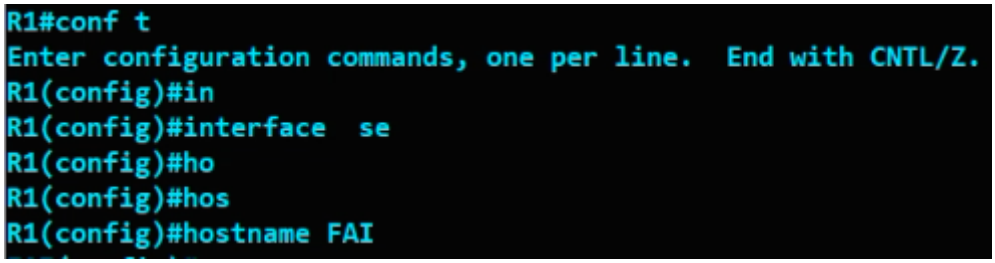


FIGURE 4.33 – renommer R1 en tant que FAI.

puis nous allons configurer l'interface serial.

```
FAI(config-if)#no shutdown
FAI(config-if)#
FAI(config-if)#ip add
FAI(config-if)#ip address 99
*Apr  6 11:53:50.106: %LINK-3-UPDOWN: Interface Serial2/0, changed state to up
*Apr  6 11:53:51.110: %LINEPROTO-5-UPDOWN: Line protocol on Interface Serial2/0, changed state to up
FAI(config-if)#ip address 99.99.99.2 255.255.255.252
FAI(config-if)#
FAI(config-if)#end
```

FIGURE 4.34 – Configuration du l'interface 2/0

Configuration du routeur RT-Dist

On va configurer l'interface serial du routeur RT-Dist.

```
RT-Dist#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
RT-Dist(config)#in
RT-Dist(config)#interface  se
RT-Dist(config)#interface  serial 2/0
RT-Dist(config-if)#no shu
RT-Dist(config-if)#no shutdown
RT-Dist(config-if)#ip add
RT-Dist(config-if)#ip address
*Apr  6 11:54:34.478: %LINK-3-UPDOWN: Interface Serial2/0, changed state to up
*Apr  6 11:54:35.478: %LINEPROTO-5-UPDOWN: Line protocol on Interface Serial2/0, changed state to up
RT-Dist(config-if)#ip address 99.99.99.1 255.255.255.252
RT-Dist(config-if)#
RT-Dist(config-if)#cl
RT-Dist(config-if)#clo
RT-Dist(config-if)#clock r
RT-Dist(config-if)#clock rate ?
  threshold  Configure the threshold clockrate limit for DTE interfaces

RT-Dist(config-if)#end
```

FIGURE 4.35 – Configuration du routeur RT-Dist

Afin de vérifier la configuration ,nous allons utiliser la commande "**show ip interface brief**"

```
R1#show  ip interface brief
Interface                  IP-Address      OK? Method Status                Protocol
Ethernet0/0                10.1.1.2        YES manual up                    up
Ethernet0/1                192.168.131.132 YES DHCP   up                    up
Ethernet0/2                unassigned      YES NVRAM  administratively down down
Ethernet0/3                unassigned      YES NVRAM  administratively down down
Ethernet1/0                unassigned      YES NVRAM  administratively down down
Ethernet1/1                unassigned      YES NVRAM  administratively down down
Ethernet1/2                unassigned      YES NVRAM  administratively down down
Ethernet1/3                unassigned      YES NVRAM  administratively down down
Serial2/0                  unassigned      YES NVRAM  administratively down down
Serial2/1                  unassigned      YES NVRAM  administratively down down
Serial2/2                  unassigned      YES NVRAM  administratively down down
 --More--
```

FIGURE 4.36 – Vérifier la configuration

4.5 Partie 1 : La supervision "Monitorig"

4.5.1 Méthodologie

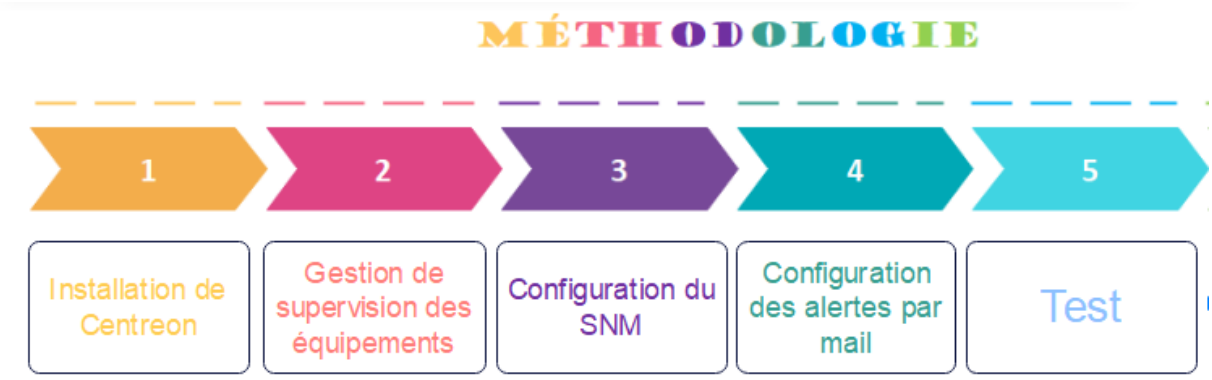


FIGURE 4.37 – Méthodologie

4.5.2 Installation de Centreon

1- Configuration de la machine virtuelle

Centreon fournit une machine virtuelle prête à l'emploi. Cette machine virtuelle est disponible au format OVA pour les environnements VMware et OVF pour l'outil Oracle VirtualBox. Elle est basée sur le système d'exploitation **Alma Linux 8** et inclut une installation de Centreon permettant de démarrer en toute simplicité votre première supervision.

La VM est configurée en **Thin Provision** pour économiser autant d'espace libre que possible sur le disque (meilleure pratique).

La machine hôte doit avoir les caractéristiques suivantes :
- **Processeur :** Tout processeur Intel ou AMD récent avec au moins 2vCPU.
- **Mémoire :** Selon nos systèmes d'exploitation, nous avions besoin d'au moins 1 Go de RAM. Pour profiter pleinement de l'expérience, nous avions besoin d'au moins 2 Go de mémoire libre.
- **Espace disque :** La machine virtuelle nécessitait au moins 6,5 Go d'espace libre sur notre disque dur. Cependant, si nous souhaitions continuer à utiliser Centreon, il était recommandé d'avoir au moins 10 Go car sa taille augmentait avec le temps.

1. Nous avons vérifié que notre solution de virtualisation (VirtualBox ou VMWare) était installée sur notre machine et à jour.
2. Nous sommes allés sur la page de téléchargement de Centreon. Dans la section 1, "Appliances" était sélectionné par défaut.
3. Dans la section 2, nous avons sélectionné la version de Centreon désirée.
4. Dans la section 3, "Download your image", nous avons cliqué sur le bouton "Download" à côté de la machine virtuelle désirée. Une nouvelle page est apparue.
   - Si nous souhaitions être contactés par Centreon, nous avons entré nos informations de contact, puis cliqué sur "Download".

— Dans le cas contraire, nous avons cliqué sur "Direct download".

5. Le fichier téléchargé était une archive compressée : nous avons extrait son contenu dans le répertoire désiré.

Installation de la machine virtuelle

1. Nous avons importé le fichier **centreon-central.ova** dans VMWare. Un terminal s'est ouvert : nous avons attendu que le serveur démarre. Lorsque celui-ci était prêt, le terminal affichait le message suivant :

Figure 4.38 – Message afficher

2. Selon la structure de notre réseau, dans la configuration de notre machine virtuelle, nous avons ajouté un adaptateur réseau et sélectionné le réseau via lequel la machine pouvait communiquer avec les ressources qu'elle devait superviser.

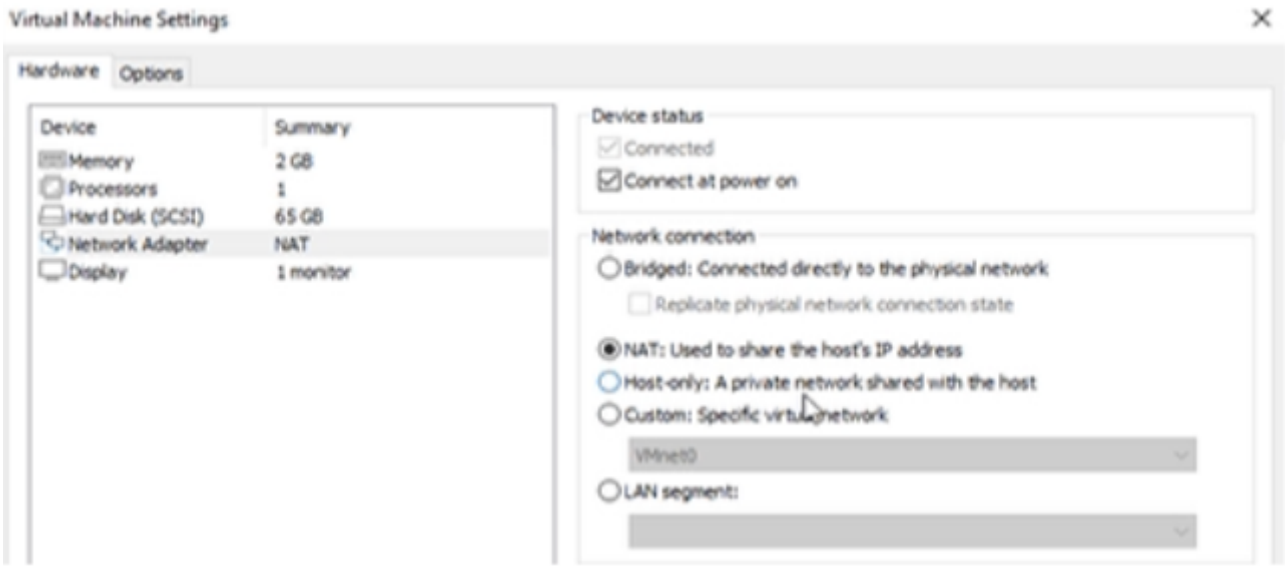


Figure 4.39 – Ajoute d'un adaptateur réseau

Pour finaliser la configuration, nous devions :

3. Nous connecter au serveur Centreon avec les informations suivantes :
   - login : root.
   - password : centreon.

4. Pour connaître l'adresse IP de notre serveur, nous avons tapé **ip addr**.
   La VM est configurée pour obtenir une adresse IP automatiquement du serveur DHCP.

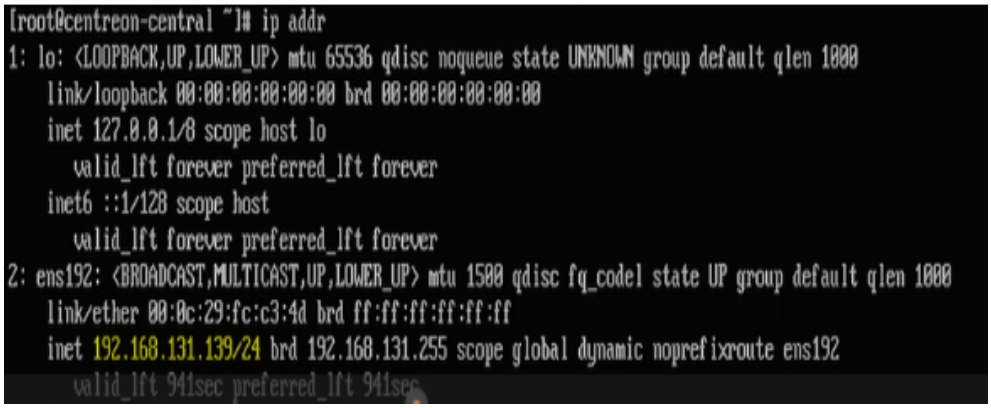


Figure 4.40 – Connaître l'adresse IP de serveur

5. Nous nous sommes connectés en tant que **root** au serveur depuis une autre machine en utilisant le terminal de notre choix, en utilisant l'adresse IP obtenue précédemment.
6. Lors de notre première connexion au serveur, des instructions se sont affichées pour nous aider à terminer la configuration.

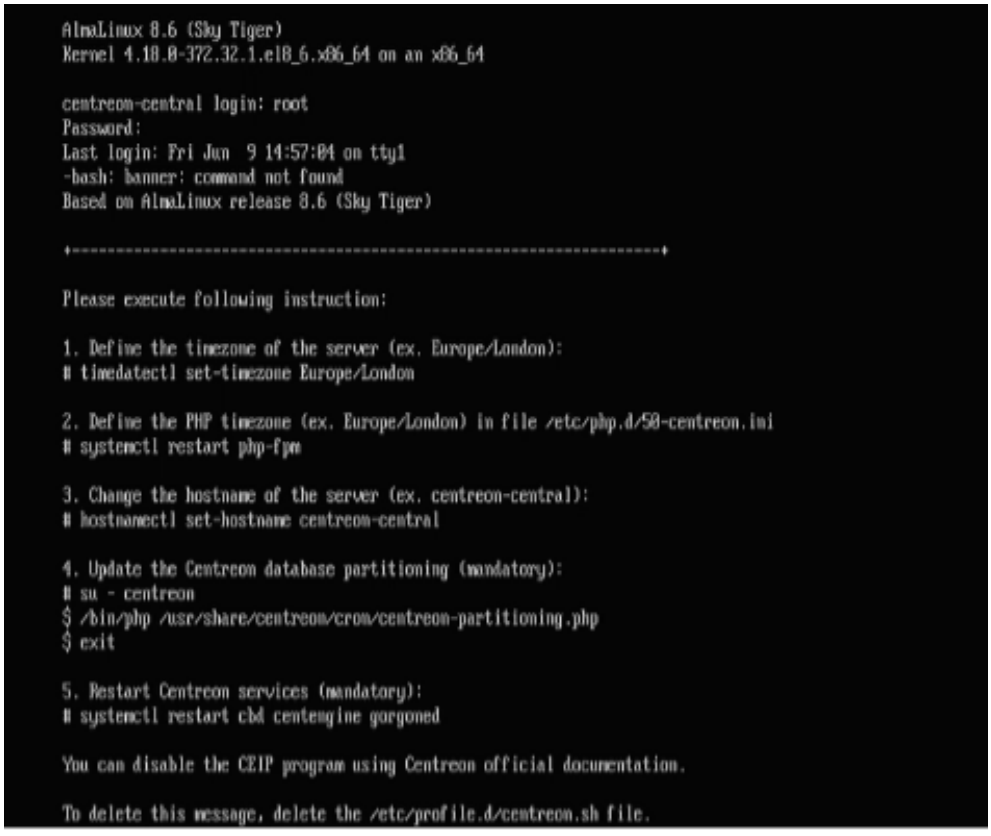


Figure 4.41 – Les instructions afficher

7. Nous avons défini les paramètres suivants :
   — Le fuseau horaire (timezone) du serveur Centreon. Par défaut, celui-ci est UTC. Cela définira l'heure des différents logs de Centreon.
   Nous avons utilisé la commande suivante

FIGURE 4.42 – Le fuseau horaire (timezone)

   — Nous avons redémarré le serveur php.

FIGURE 4.43 – Redémarrage de serveur php

   — Le hostname de notre serveur (facultatif). Le nom par défaut du serveur était centreon-central. Par exemple, si nous souhaitions renommer la machine en "supervision", nous avons saisi :

FIGURE 4.44 – Renommer la machine supervision

8. Nous avons ajouté une partition pour la table MariaDB. Cette étape était obligatoire. Votre serveur ne fonctionnerait pas si vous ne l'aviez pas exécutée.
   — Connectez-vous en tant que l'utilisateur **centreon** :

FIGURE 4.45 – Connexion en tant que l'utilisateur : centreon

   — Nous avons entré la commande suivante :

   — Nous nous sommes reconnectés à nouveau en tant qu'utilisateur**root** :

FIGURE 4.46 – Connexion en tant que l'utilisateur : root

— Nous avons redémarré le processus Centreon broker pour que les changements soient appliqués :

```
[root@centreon-central ~]# systemctl restart cbd centengine gorgoned
```

FIGURE 4.47 – Redémarrage du processus Centreon

Notre serveur Centreon est maintenant prêt à l'emploi.

9. Nous nous sommes connectés à l'interface web. Dans notre navigateur, nous avons saisi l'adresse du serveur au format requis**http ://addresse_ip/centreon** ou **http ://FQDN/centreon**. (Par exemple, une URL valide avec notre add ip **http ://192.168.131.139/centreon**.)
10. Nous nous sommes connectés en utilisant les informations suivantes : Login : **admin**. Password :**Centreon!123**.
    Par défaut, notre serveur offre une configuration prédéfinie qui permet de le superviser lui-même.

La figure ci-dessus représente l'interface de connexion de l'application

FIGURE 4.48 – Interface d'authentification de Centreon.

4.5.3 Gestion de supervision des équipements

Pour superviser les équipements de notre architecture comprenant des serveurs Windows/Linux, des commutateurs et des routeurs, il est nécessaire d'installer et de configurer le service SNMP sur chaque hôte. Les étapes suivantes décrivent la procédure à suivre pour réaliser cette supervision, illustrées par des figures explicatives.

Supervision du serveur windows :

Sur le serveur Windows que vous souhaitez superviser

La première étape consiste à installer le service SNMP sur l'hôte Windows.

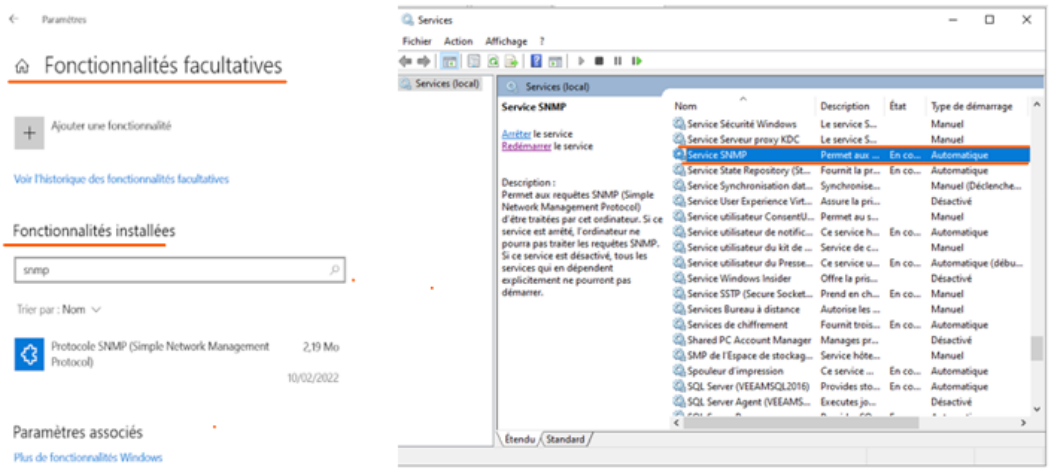


FIGURE 4.49 – Installation du service SNMP

Maintenant on va passer à la configuration du service pour ce faire , on doit d'abord créer un agent et ajouter une communauté pour permettre son interrogation.

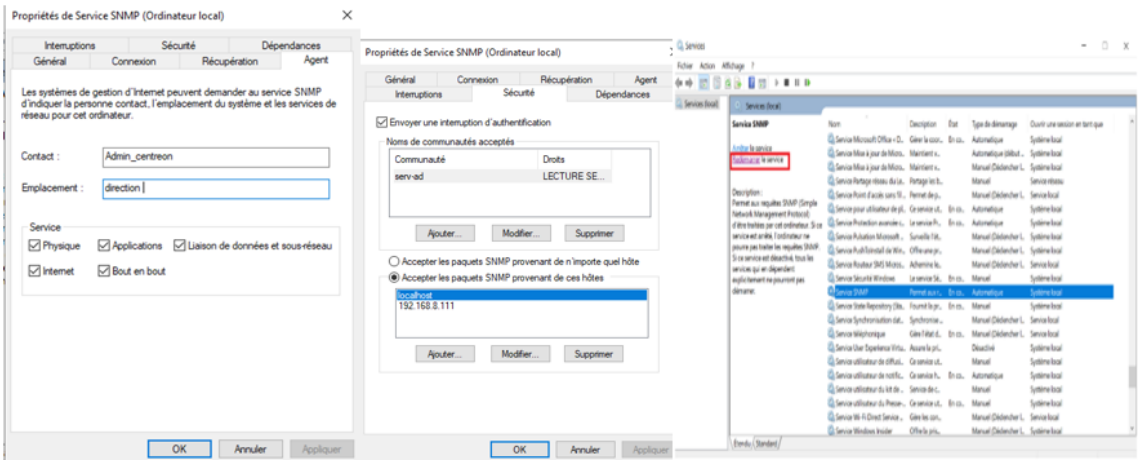


FIGURE 4.50 – Configuration du service

Sur le serveur Centreon (collecteur)

Sur ce serveur nous devons installer le plugin SNMP avec la commande illustré dans la figure suivante :

```
[root@supervision ~]# dnf install centreon-plugin-Operatingsystems-Windows-Snmp
Last metadata expiration check: 1:49:51 ago on Fri 09 Jun 2023 04:12:47 PM CET.
Package centreon-plugin-Operatingsystems-Windows-Snmp-20221017-094659.el8.noarch is already installed.
Dependencies resolved.
================================================================================
 Package                                  Architecture Version                 Repository                Size
================================================================================
Upgrading:
 centreon-plugin-Operatingsystems-Windows-Snmp
                                          noarch       20230608-122119.el8     centreon-stable-noarch    89 k

Transaction Summary
```

FIGURE 4.51 – Installation du plugin SNMP réussie

Sur le serveur Centreon (central)

Dans cette étape, nous accédons à l'interface Web comme nous l'avons expliqué précédemment. Tout d'abord, nous nous rendons sur la section Configuration > Plugin Packs et nous installons le Plugin Pack Windows SNMP. Une fois le plugin installé, nous passons à l'étape suivante qui consiste à remplir le formulaire d'ajout de notre équipement. Pour ce faire, nous suivons les instructions suivantes :

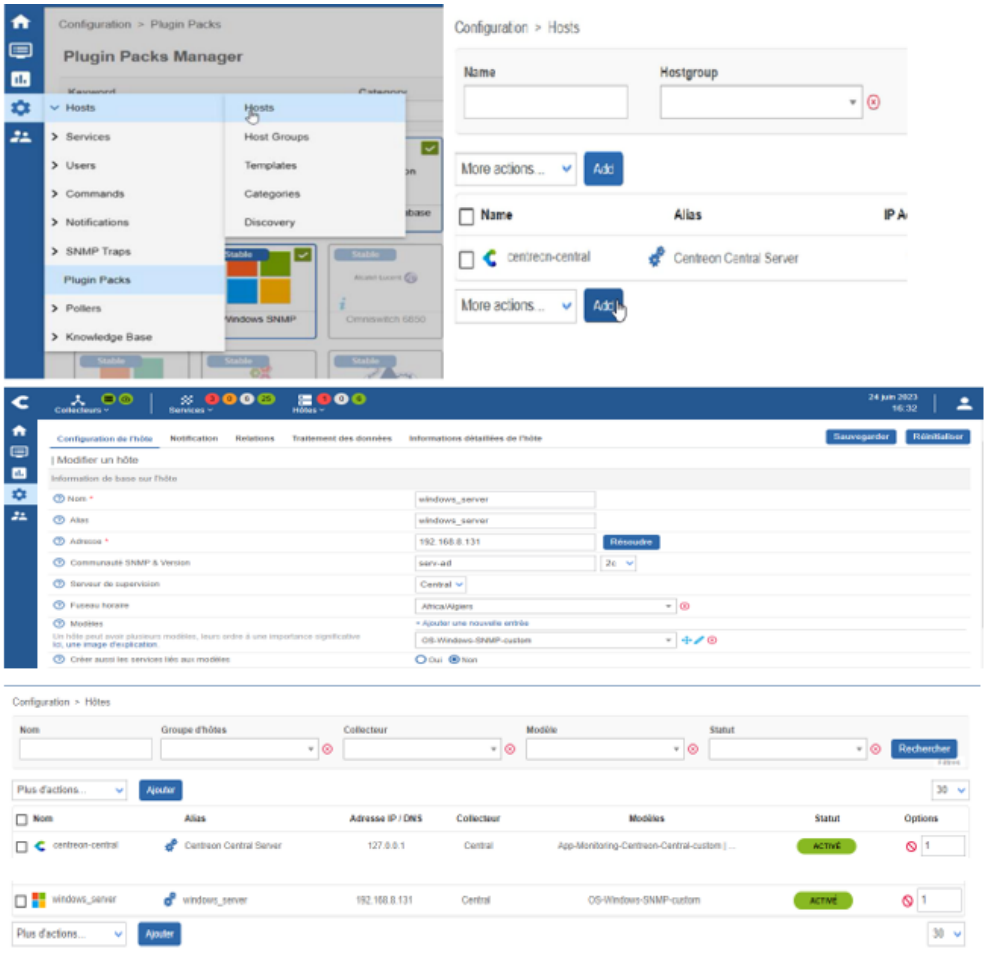


FIGURE 4.52 – Ajout du serveur Windows sur Centreon

Configuration des services

Le service peut être basé sur un modèle comme pour les hôtes, il est lié à un hôte ou à un groupe d'hôtes.

Un service intègre une commande (commande qui permet la vérification d'un état) avec ses arguments.

Initialement pour effectuer l'ajout d'un service on doit se rendre sur Configuration> Services > Services par hôtes, puis on clique sur Ajouter , ensuite sur le formulaire d'ajout nous devons choisir l'équipement au quel nous voudrions ajouter ce service , la figure suivante explique les démarches à suivre :

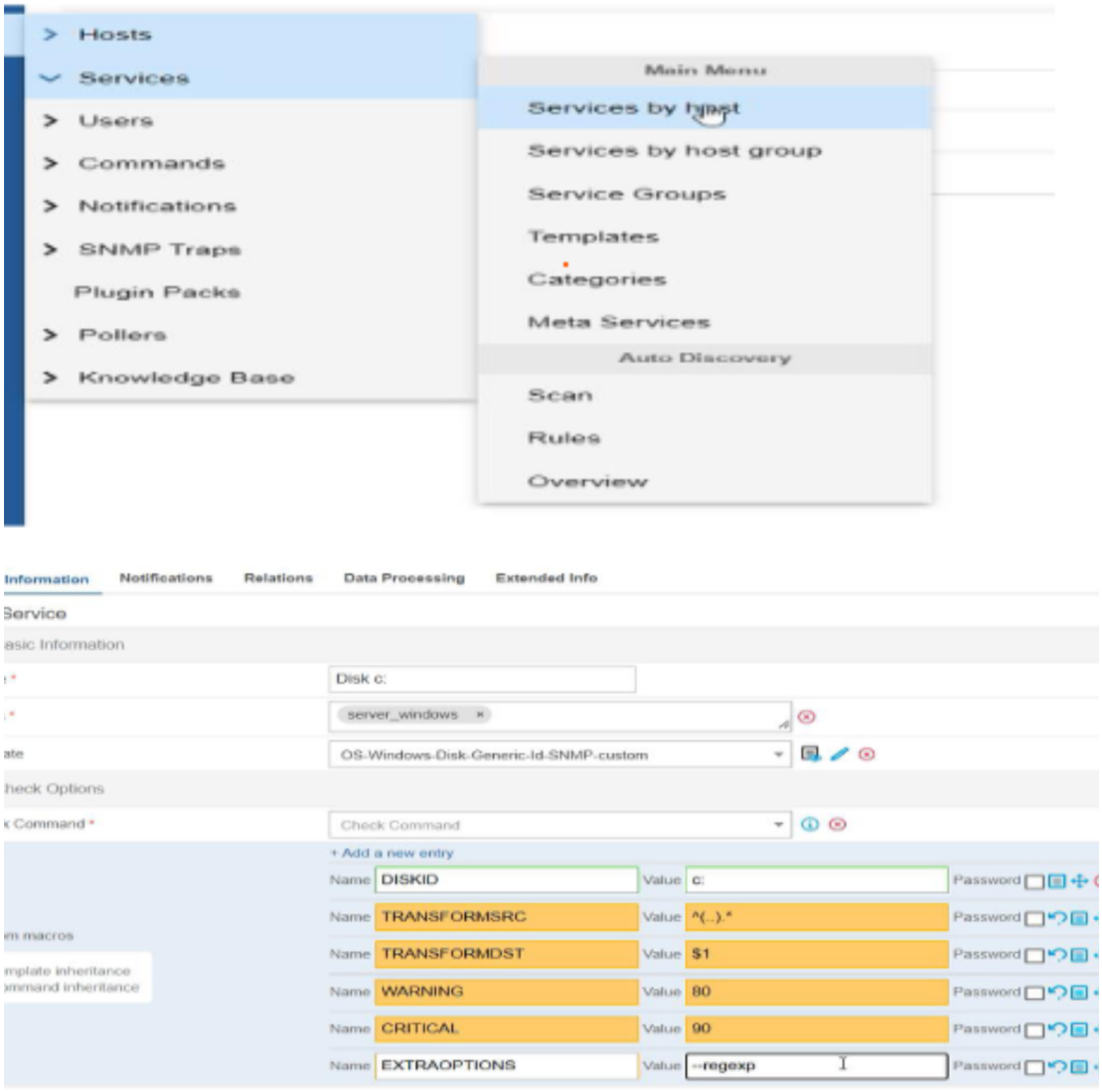


FIGURE 4.53 – Formulaire d'ajout de service disk C

Le disk c est ajouter avec succès.

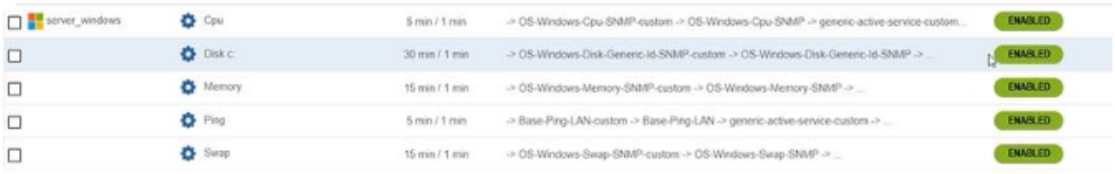


FIGURE 4.54 – service disk c ajouté avec succès au serveur windows

Ajout du switch Core1

Avant d'ajouter un commutateur et un routeur, il est nécessaire de se rendre sur la console de GNS3 afin de configurer l'agent SNMP, créer une communauté et définir ses droits.

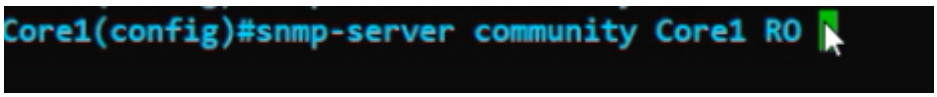


FIGURE 4.55 – Création d'une communauté et définir ses droits.

Après cela, il est nécessaire de remplir le formulaire d'un hôte sur Centreon, tel qu'illustré dans la figure ci-dessous.

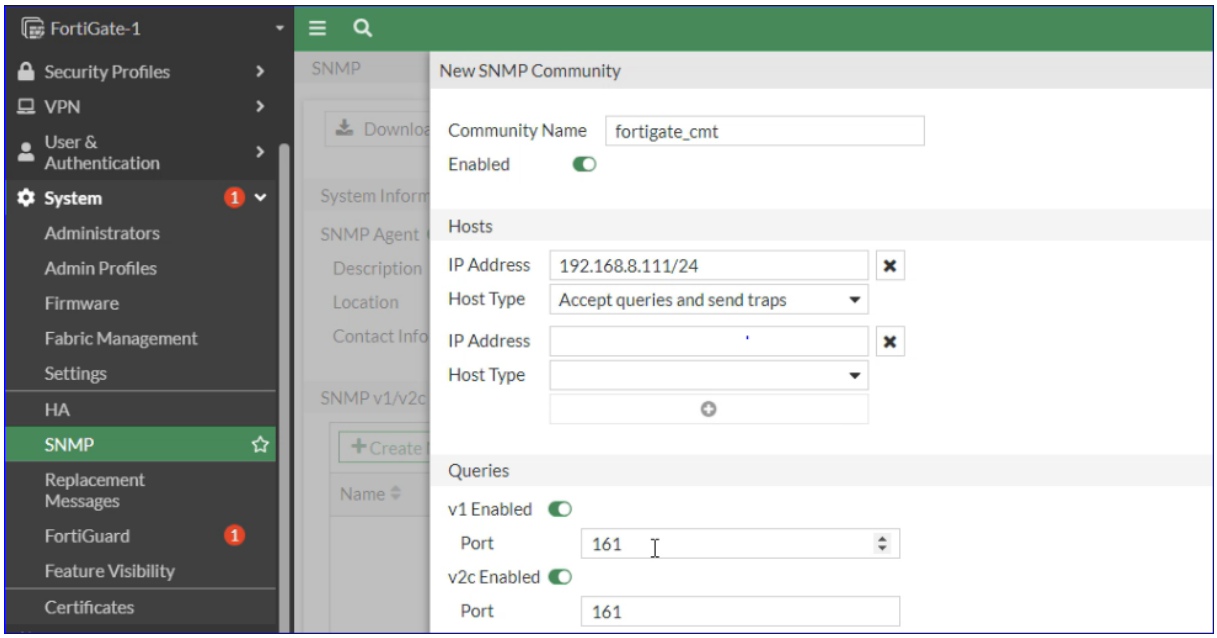


FIGURE 4.56 – Formulaire d'ajout du switch Core1

Ajout d'un switch d'accès

Pour ajouter un switch d'accès, nous devons suivre le même processus que celui mentionné précédemment pour l'ajout du switch Core .

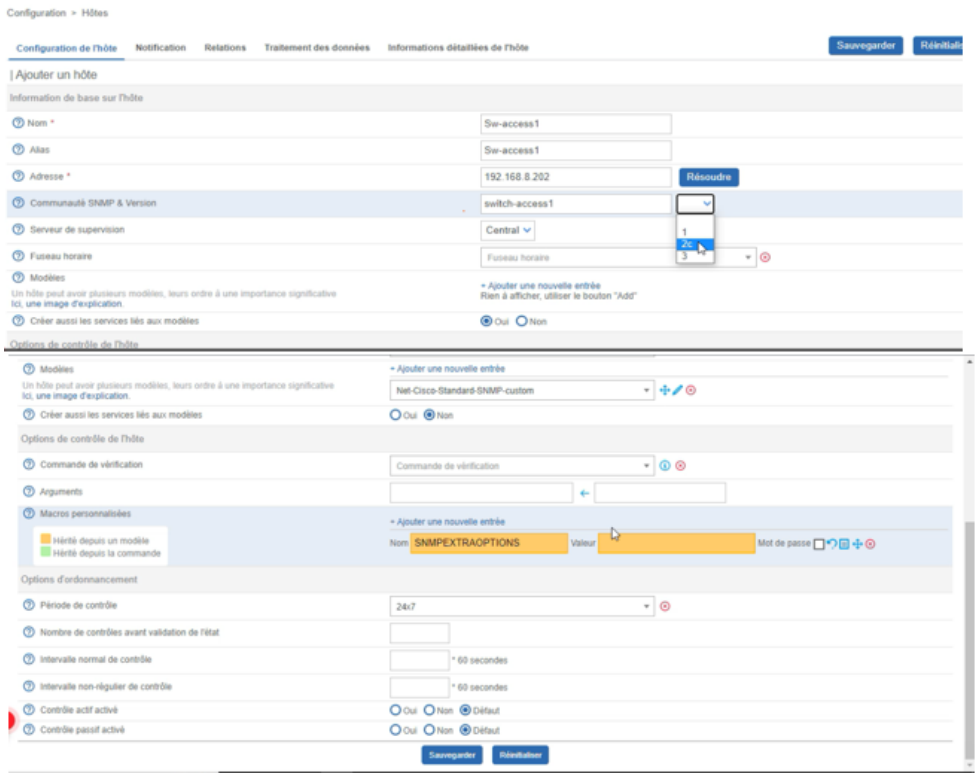


FIGURE 4.57 – Formulaire d'ajout du switch d'accès 1

Ajout du pare-feu Forti-Gate

Avant de commencer on doit activer le protocole SNMP sur le pare-feu Forti-Gate, l dans le menu **"Système"** > **"SNMP"**, puis **enable " Agent SNMP"** et dans ce cas nous permettrons v2c, nous le faisons en cliquant sur "Créer un nouveau".

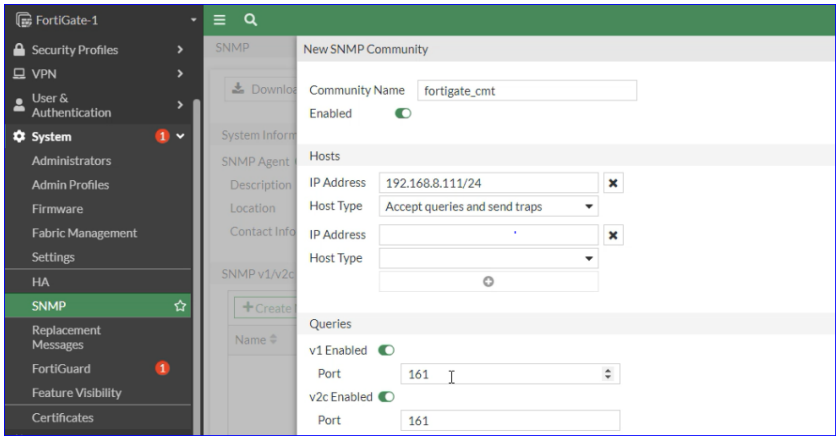


FIGURE 4.58 – Activation du protocole SNMP sur Forti-Gate

Installation du plug-in pour surveiller Forti-Gate

Nous devons procéder à l'installation du plug-in Forti-Gate en créant des scripts, car le plug-in Forti-Gate sur Centreon est payant. Les étapes détaillées dans les figures suivantes Les figures suivantes expliqueront toutes les étapes à suivre pour son installation.

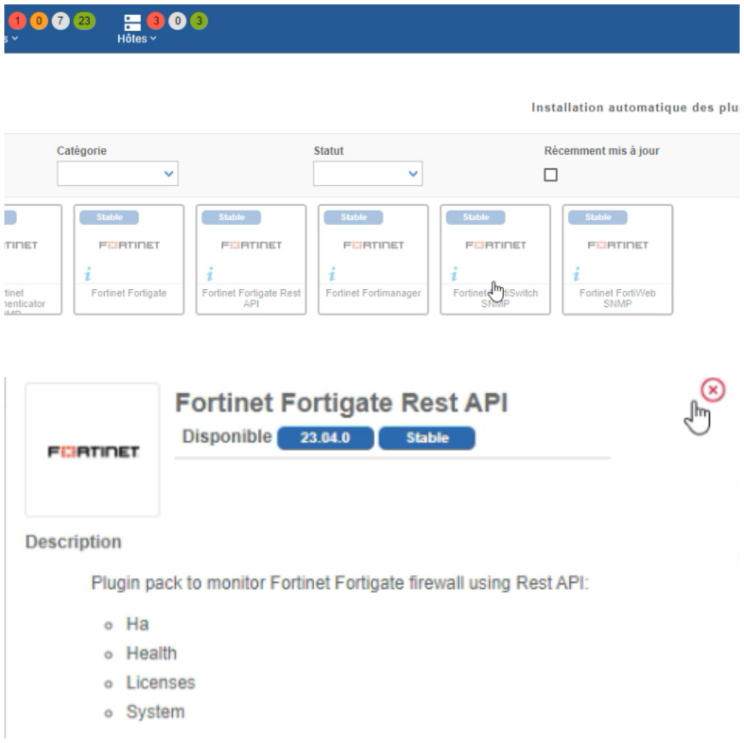


FIGURE 4.59 – plugin Forti-Gate exige un abonnement

téléchargements des packages .

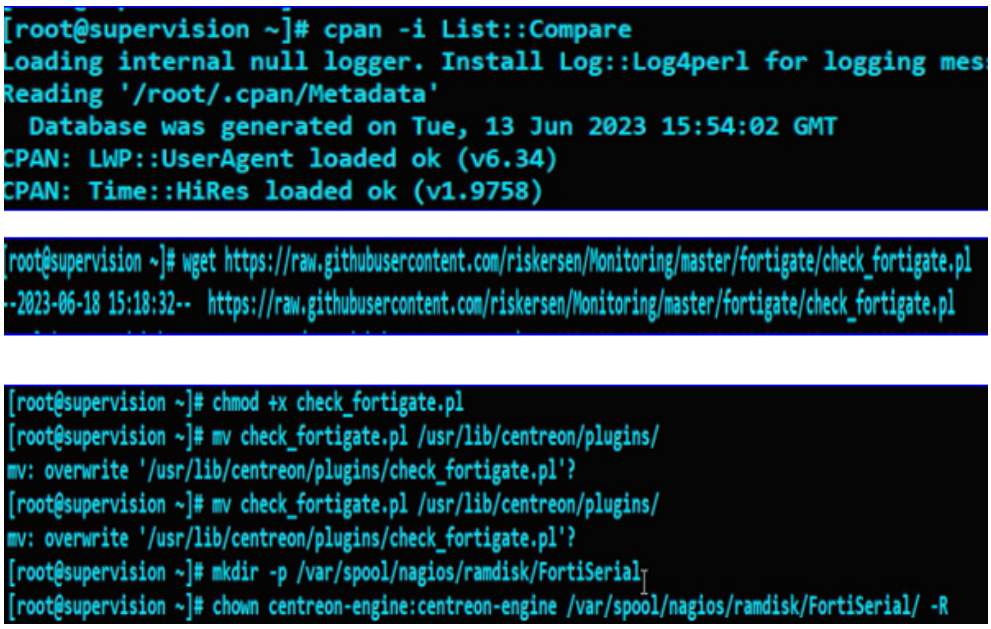


FIGURE 4.60 – téléchargements des packages

Commandes permettant d'exécuter les package téléchargés de FortiGate .

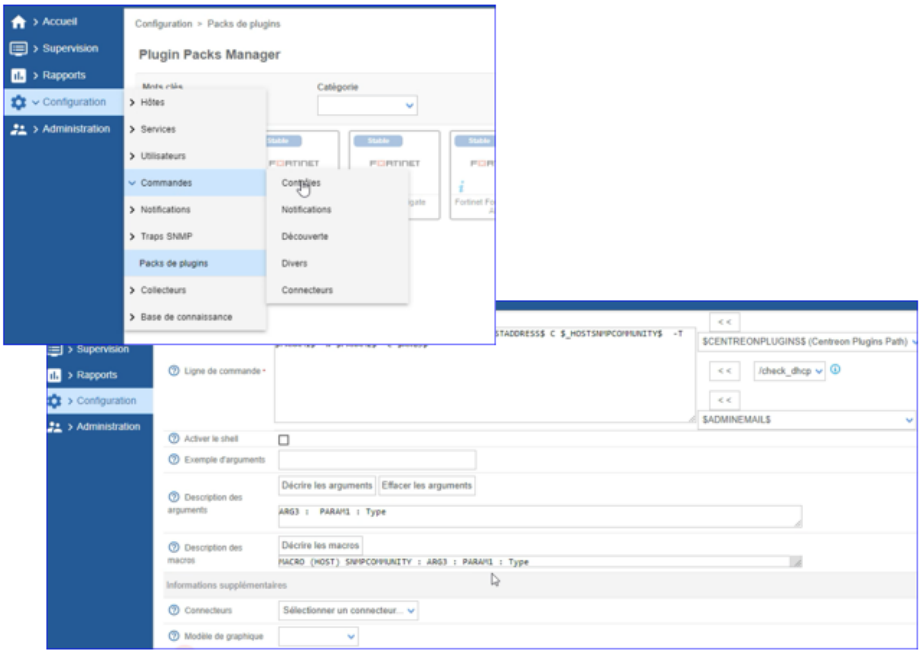


FIGURE 4.61 – Commandes permettant d'exécuter les package téléchargés de Forti-Gate

Création de l'hôte et services forti-gate .

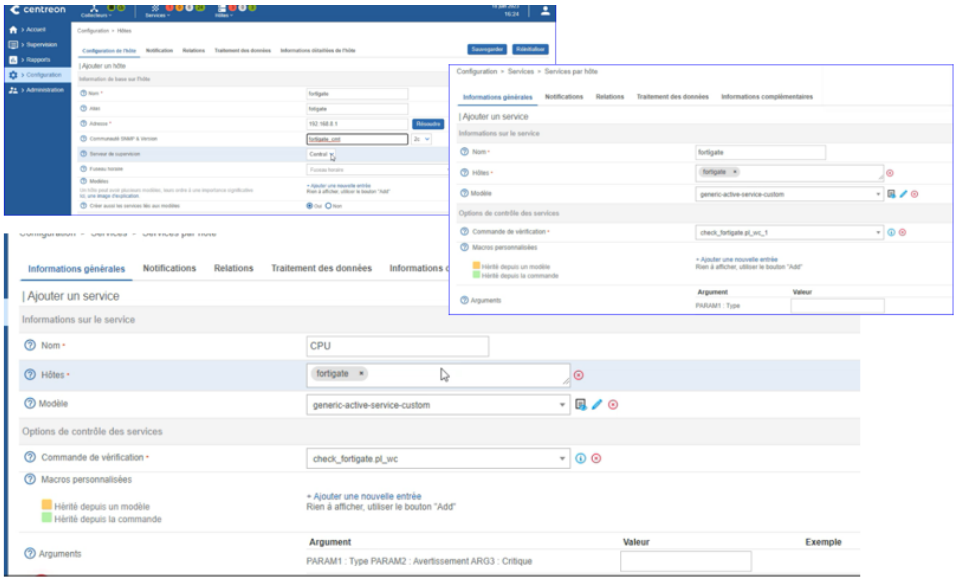


FIGURE 4.62 – Création de l'hôte et services fortigate

Déployer une configuration

Lorsque nous créons, supprimons ou modifions des hôtes et services à partir du menu Configuration, les changements effectués ne sont pas appliqués automatiquement. Cela s'applique aussi bien au serveur central sur lequel nous avons effectué les modifications qu'à tout collecteur ou serveur distant qui en dépendrait. Afin que les modifications soient prises en compte, il est nécessaire d'exporter la configuration.

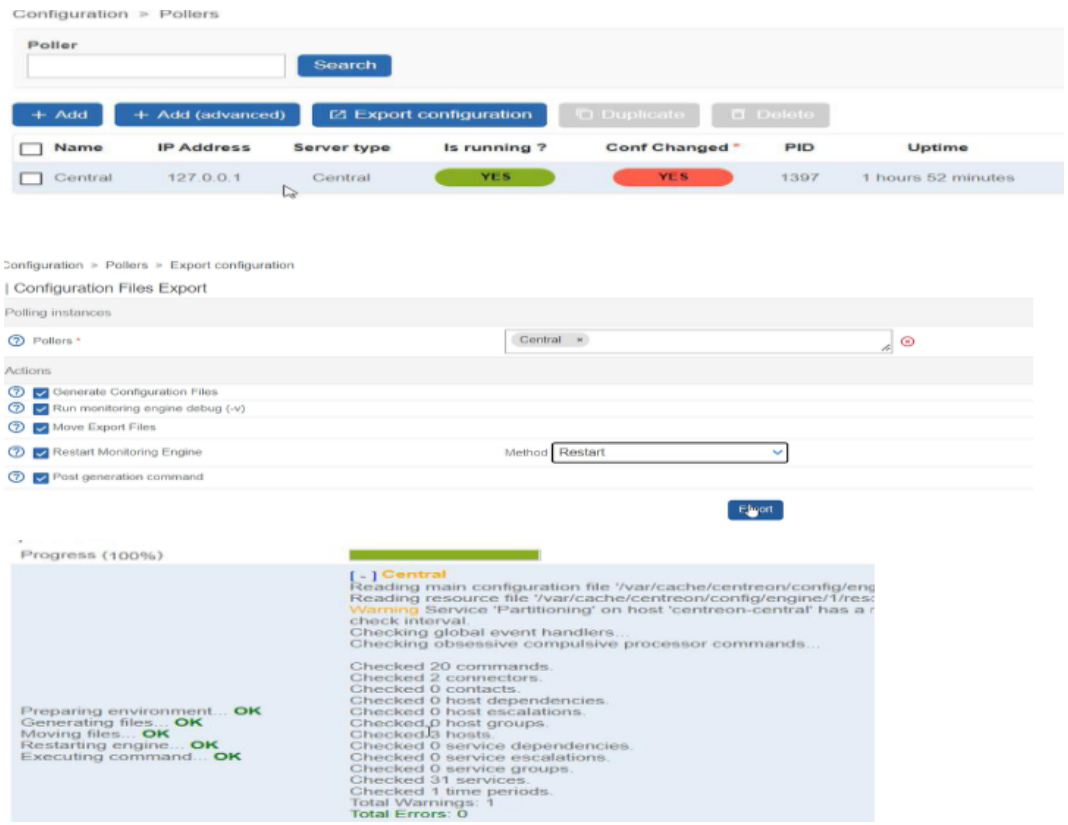


FIGURE 4.63 – Création de l'hôte et services fortigate

4.5.4 Configuration du SNMPv3

En configurant SNMPv3 avec une ACL nous pouvons collecter des informations précieuses sur les performances du réseau, les erreurs, les statistiques de trafic, etc., tout en maintenant un niveau élevé de sécurité, les figures suivantes détaillerons les étapes de cette configuration.

1. Dans une première partie nous devons créer une ACL.
   Nous devons se rendre sur le routeur qu'on souhaite configurer avec SnmpV3.

```
R1(config)#ip access-list standard centreon-acl
R1(config-std-nacl)#permit host 192.168.8.111
R1(config-std-nacl)#exit
```

FIGURE 4.64 – Création d'une ACL

2. Configuration du SnmpV3 .

```
R1(config)#snmp-server group group4 v3 priv access centreon-acl
```

FIGURE 4.65 – Configuration du SnmpV3

3. sur interface de centreon nous aller ajouter les identifiant.

FIGURE 4.66 – configuration du SNMPV3 sur centreon

4. Maintenant on va passer à l'ajout de notre routeur sur centreon .

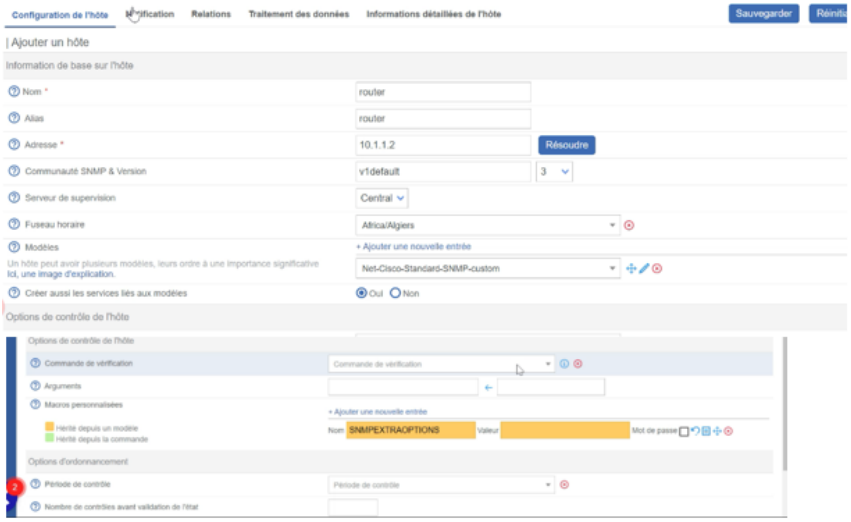


FIGURE 4.67 – Ajout du retour

5. Création d'un utilisateur et spécification de notification pour contrôler l'état du routeur

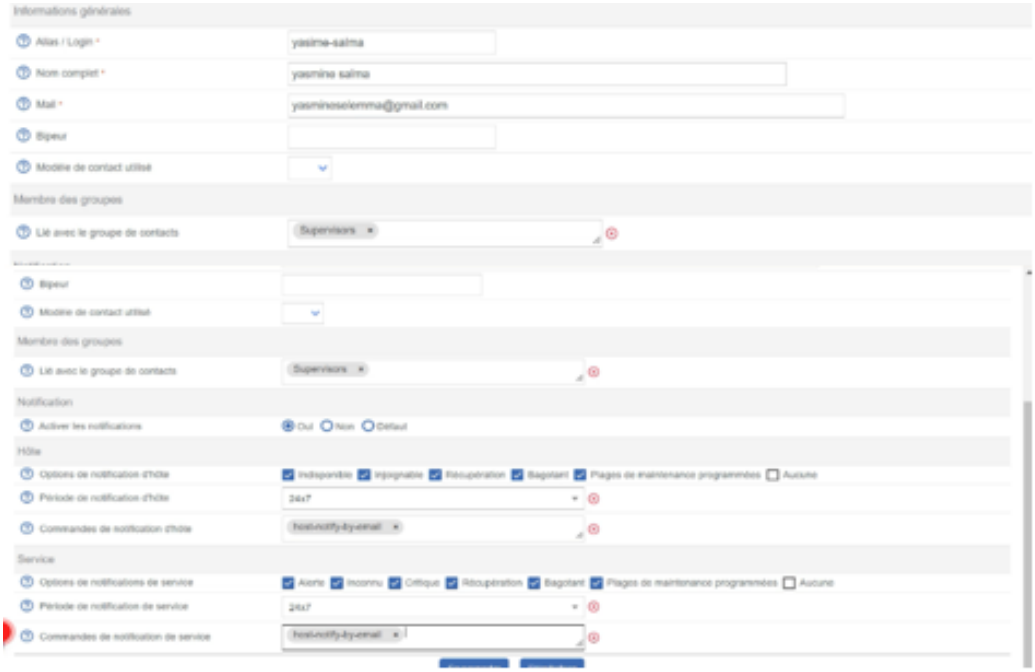


FIGURE 4.68 – création d'un utilisateur et spécification de notification pour contrôler l'état du routeur

6. Routeur Snmpv3 supervisé avec succès .

FIGURE 4.69 – Routeur Snmpv3 supervisé avec succès

4.5.5 Configuration des alertes par mail

Pour assurer une surveillance proactive et une réaction rapide aux incidents, il est nécessaire de configurer les alertes par courrier électronique dans Centreon. Pour ce faire, nous présentons les étapes dans les figures suivantes .

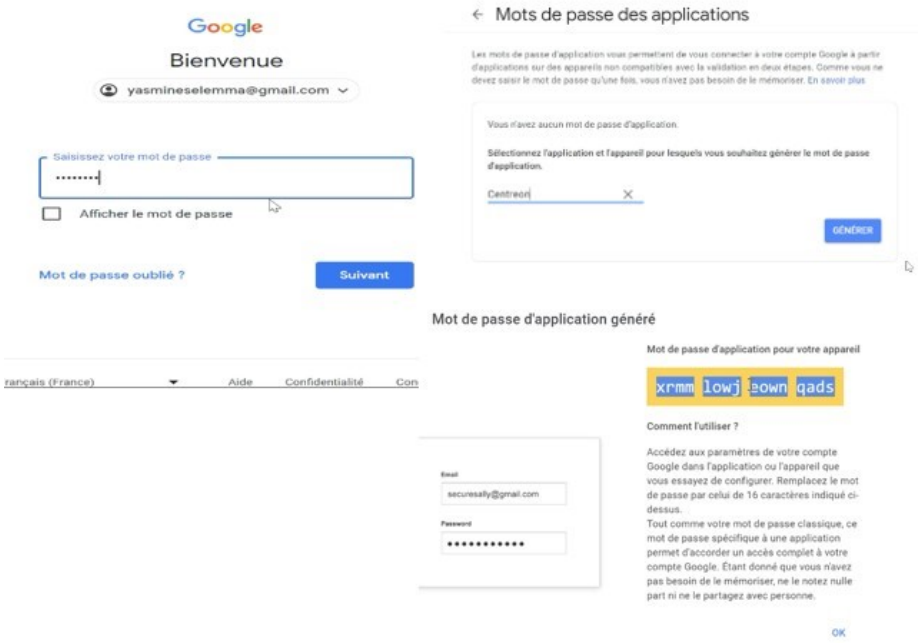


FIGURE 4.70 – Création de notre propre et génération du code

Création du contact yasmine-selma .

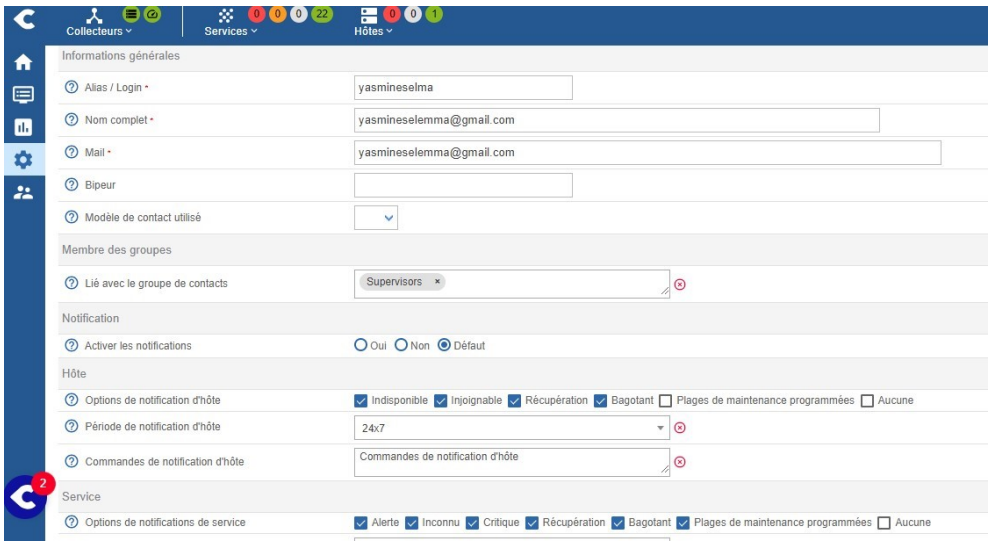


FIGURE 4.71 – Création du contact yasmine-selma

Modification des notifications .

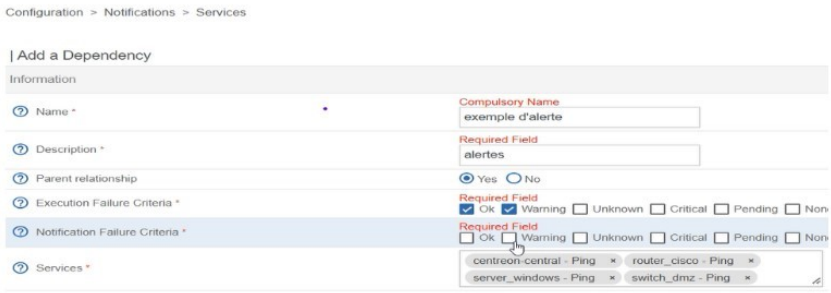


Figure 4.72 – Modification des notifications

Pour envoyer les notifications par email depuis centreon vers le serveur de messagerie il faut installer l'outil correspond : Postifx .

1. Installer Postifx en tapant cette commande dans le terminal de notre serveur

```
rpm -qa | grep postfix
sudo yum install postfix
```

Figure 4.73 – Instalation de postfix

2. Redémarrer Postifx .

```
root@sup-centreon ~]# systemctl restart postfix
```

Figure 4.74 – Redémmarage de postfx

3. Configurer Postifx pour qu'il exécute au démarrage .

```
[root@sup-centreon ~]# systemctl enable postfix
Created symlink /etc/systemd/system/multi-user.target.wants/postfix.service → /usr/lib
/systemd/system/postfix.service.
[root@sup-centreon ~]#
```

Figure 4.75 – Configuration de postfix

4. Ajout des informations néccessaires

```
myhostname = sup-centreon
relayhost = [smtp.gmail.com]:587
smtp_use_tls = yes
smtp_sasl_auth_enable = yes
smtp_sasl_password_maps = hash:/etc/postfix/sasl_passwd
smtp_tls_CAfile = /etc/ssl/certs/ca-bundle.crt
smtp_sasl_security_options = noanonymous
smtp_sasl_tls_security_options = noanonymous
```

Figure 4.76 – Ajout des informations

Ensuite nous procédons à la configurations des identifiants du compte sera utilisé pour l'envoie des e-mails.

1. Créer le fichier suivant.

```
[root@sup-centreon ~]# nano  /etc/postfix/sasl_passwd
```

Figure 4.77 – Création du fichier

2. Changer les permissions .

```
root@sup-centreon ~]#
root@sup-centreon ~]# postmap /etc/postfix/sasl_passwd
root@sup-centreon ~]#
root@sup-centreon ~]# chown root:postfix /etc/postfix/sasl_passwd*
root@sup-centreon ~]# chmod 640 /etc/postfix/sasl_passwd*
```

Figure 4.78 – Changement des permission

3. Recharger postfix .

```
root@sup-centreon ~]# systemctl reload postfix
```

Figure 4.79 – Rechargement du postfix

4.5.6 Test

Après avoir valider la configuration, notre architecture est maintenant supervisée et nous pouvons observer l'état de chaque ressource :

1. Test postfix .

```
[root@sup-centreon ~]# echo "Test" | mail -s "Test" yasmineselemma@gmail.com
```

FIGURE 4.80 – Notre émail du test

2. Résultat du test .

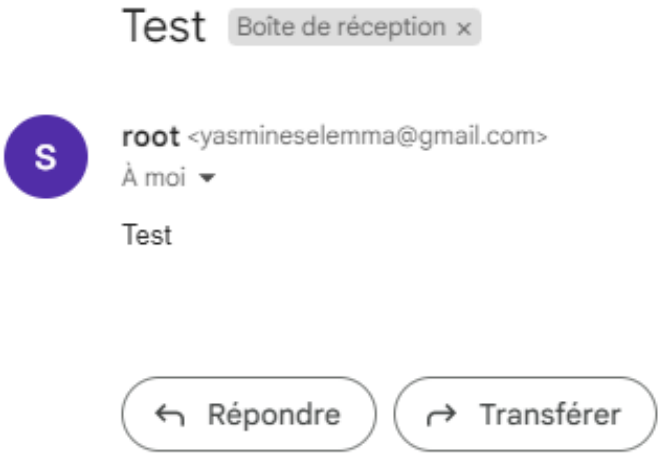


FIGURE 4.81 – Réception d'un mail de test

3. La solution a bien détecté les problèmes sur notre topologie et une alerte bien reçue par l'utilisateur.

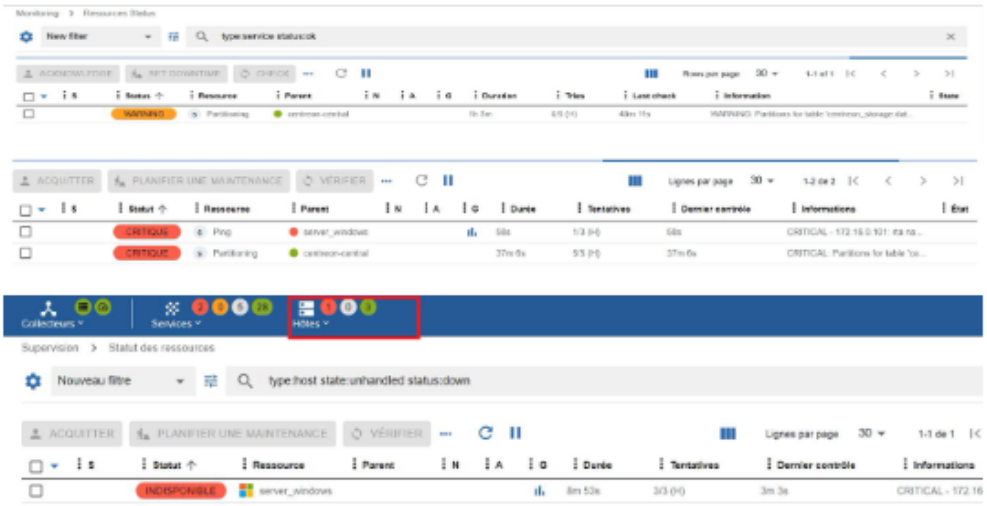


FIGURE 4.82 – Détection des problèmes

4. Alerte de type problème pour un service Swap .

FIGURE 4.83 – Alerte de type problème pour un service Swap

5. Alerte critique pour l'hôte windows server .

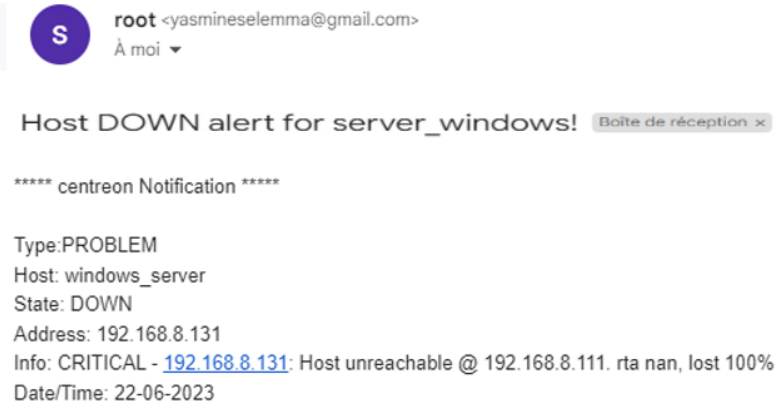


FIGURE 4.84 – Alerte critique pour l'hôte windows server

6. Après la résolution des problèmes.

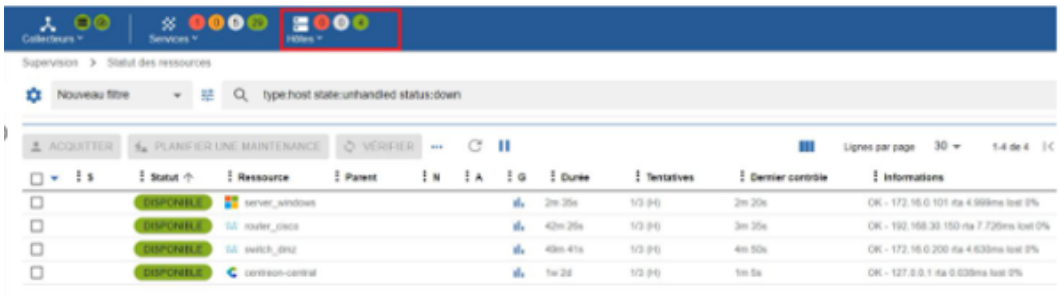


FIGURE 4.85 – Problème résolu

7. Retour service Swap en status OK.

FIGURE 4.86 – Retour service Swap en status OK

8. Retour windows en status OK.

FIGURE 4.87 – Retour windows en status OK

9. Et on terminera par un petit graphe d'un service de serveur windows.

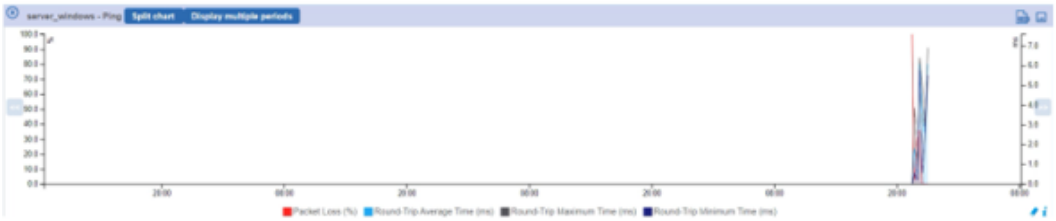


FIGURE 4.88 – Graphe de surveillance

4.6 Partie 2 : La sauvegarde "Backup" et La réplication"Reckup"

4.6.1 Méthodologie

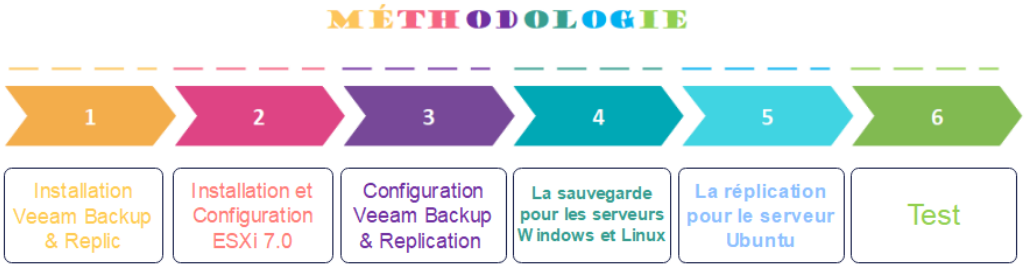


FIGURE 4.89 – Méthodologie

4.6.2 Installation Veeam Backup & Replication

1. Nous avons téléchargé la solution Veeam Backup & Replication depuis le site de Veeam. Si nous n'avions pas de compte, il était nécessaire de créer un (celui-ci était gratuit).

   Le fichier se présentait sous la forme d'une image disque au format ISO. Après l'avoir transférée sur notre serveur, nous avons sélectionné le lecteur CD de la machine puis choisi l'image.

   Dans la machine, nous avons pu lancer l'installeur. Nous avons alors sélectionné Veeam Backup & Replication Install.

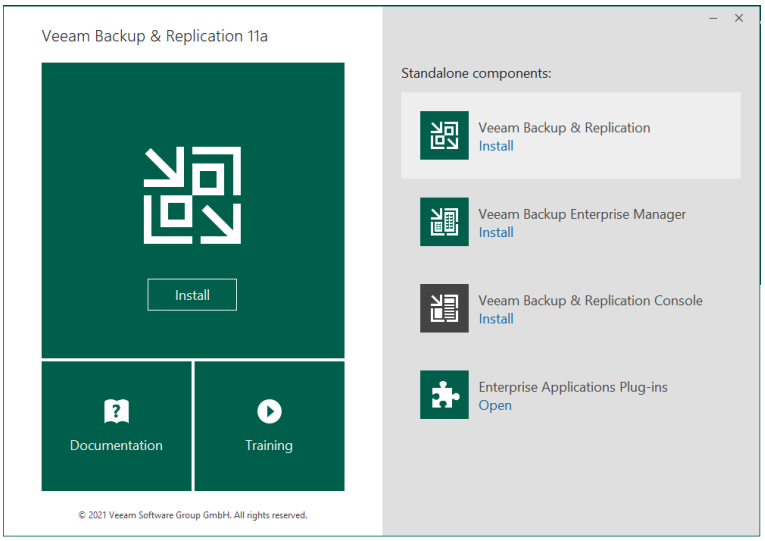


FIGURE 4.90 – Lancement de l'installation

2. Après l'avoir lu, nous avons accepté le contrat de licence en choisissant Next.

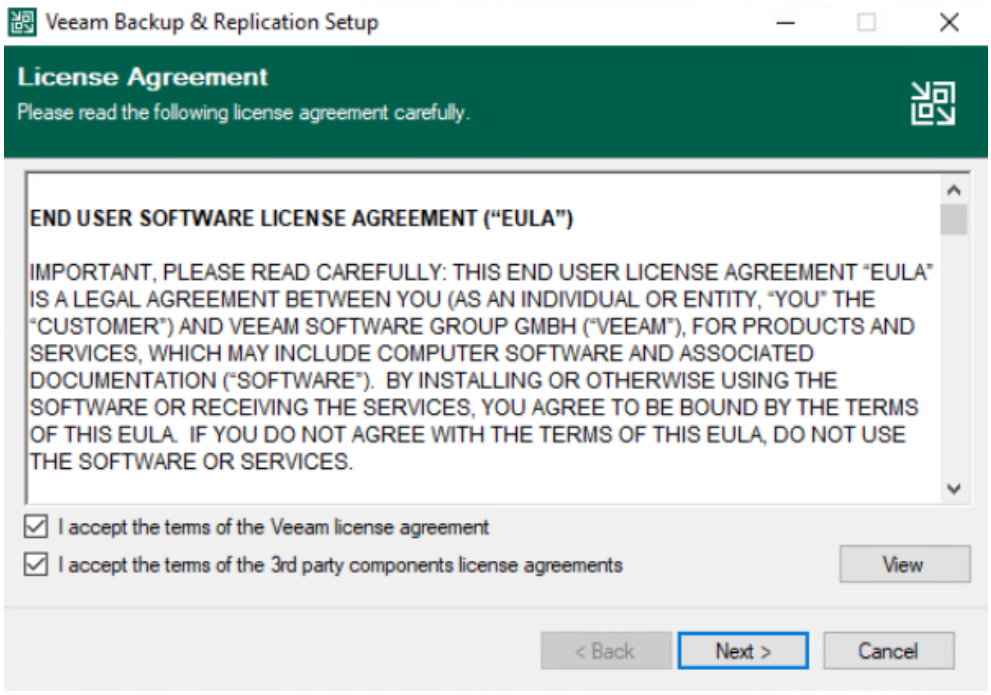


FIGURE 4.91 – Acceptation le contrat de licence

3. Nous avons passé l'étape de renseignement du fichier de licence en choisissant Next.

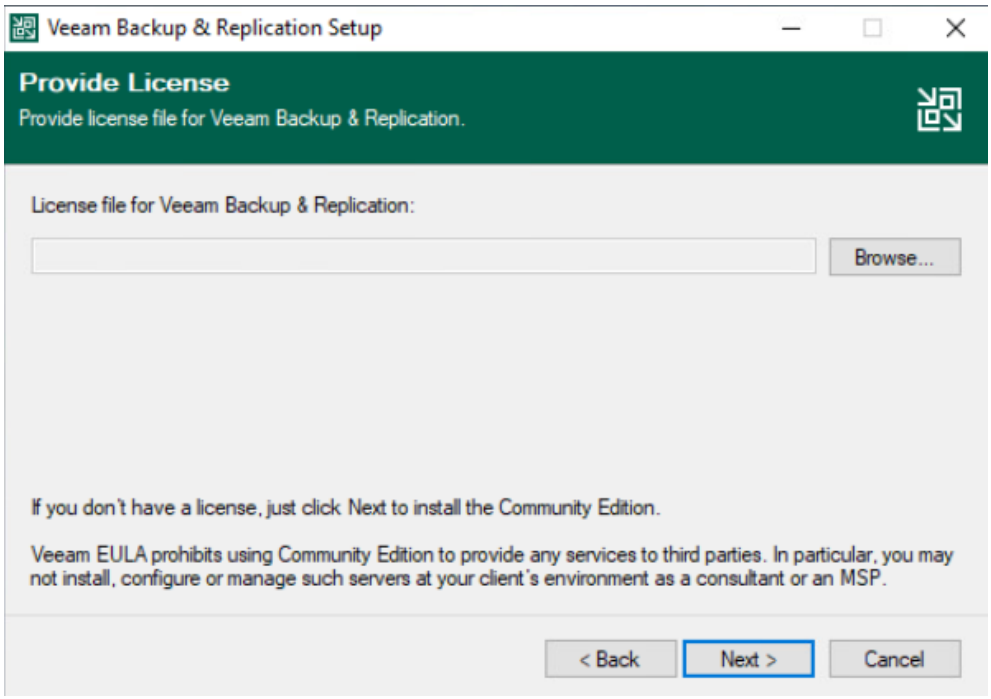


FIGURE 4.92 – Renseignement du fichier de licence

4. L'installateur a maintenant effectué un contrôle des prérequis. Comme nous partons d'une installation brute de Windows, certains composants étaient absents. Cependant, l'installeur a téléchargé et installé automatiquement ces composants manquants. Nous avons ensuite validé avec Next.

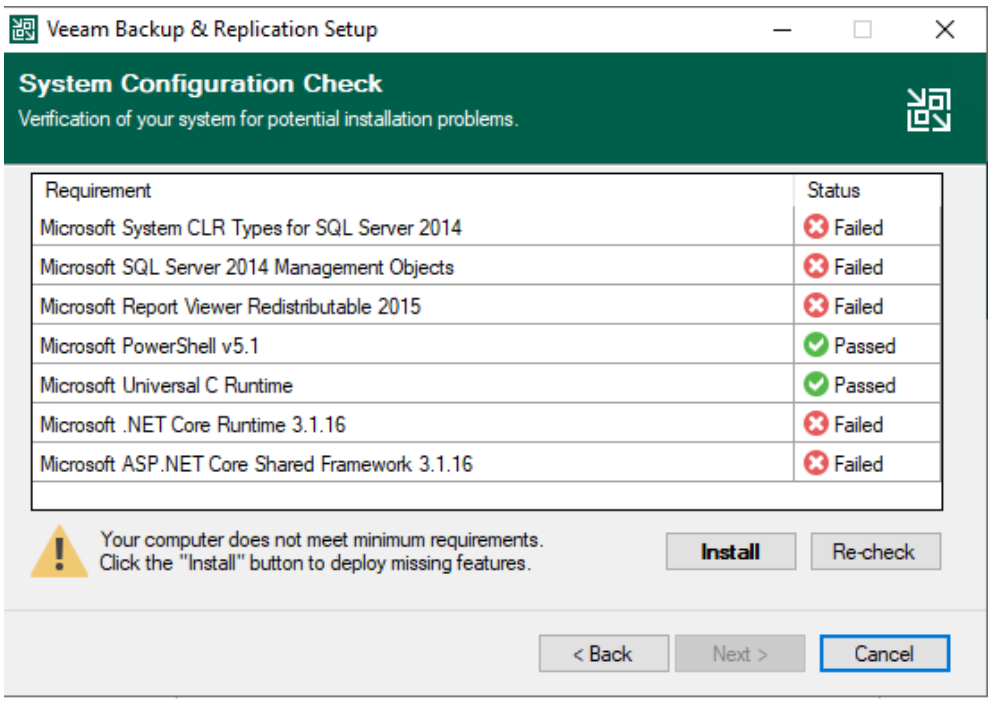


FIGURE 4.93 – Validation avec Next

5. Lors de l'étape de personnalisation de l'installation, nous avons validé l'opération en choisissant Install.

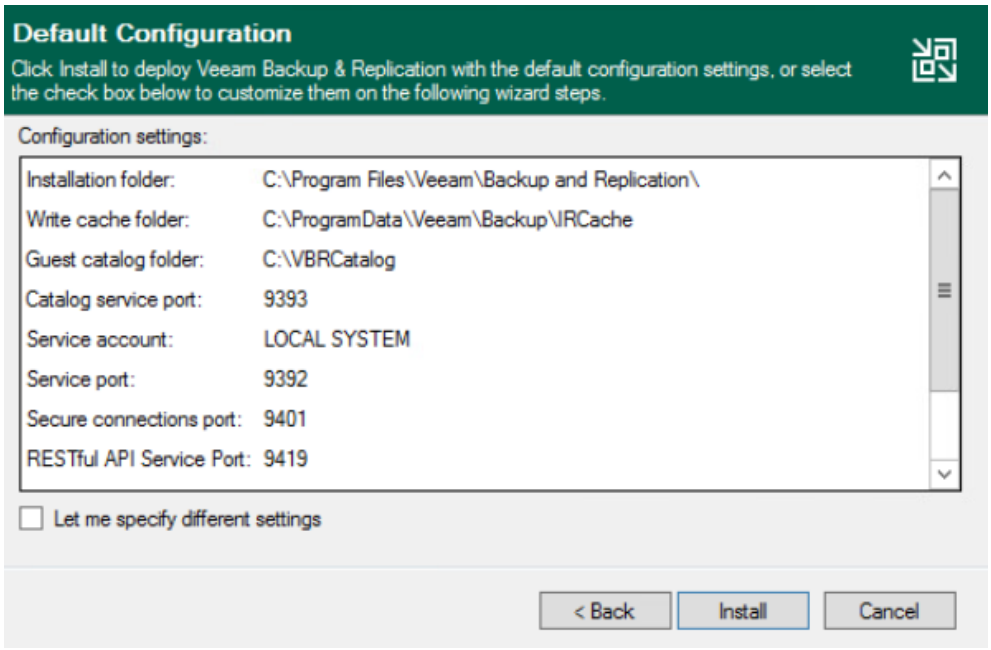


FIGURE 4.94 – Validation de l'opération

6. Une fois celle-ci terminée, quittez l'installateur en cliquant sur Finish.

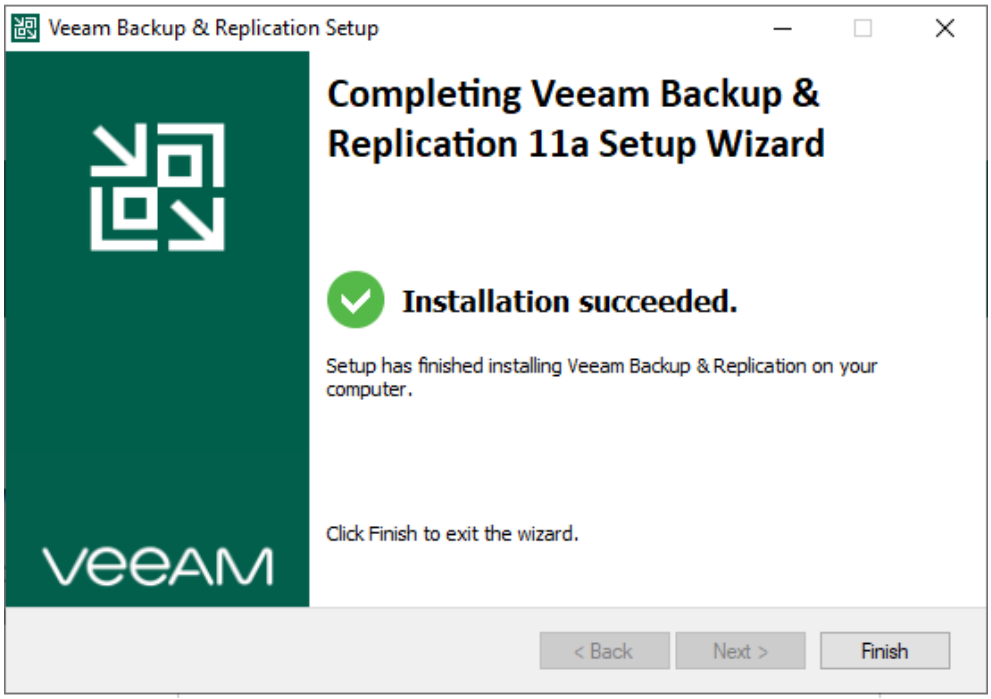


FIGURE 4.95 – Installation terminer

4.6.3 Installation ESXi 7.0

L'ajout d'une nouvelle machine virtuelle

1. Nous avons lancé VMware Workstation et cliqué sur "Nouvelle machine virtuelle".

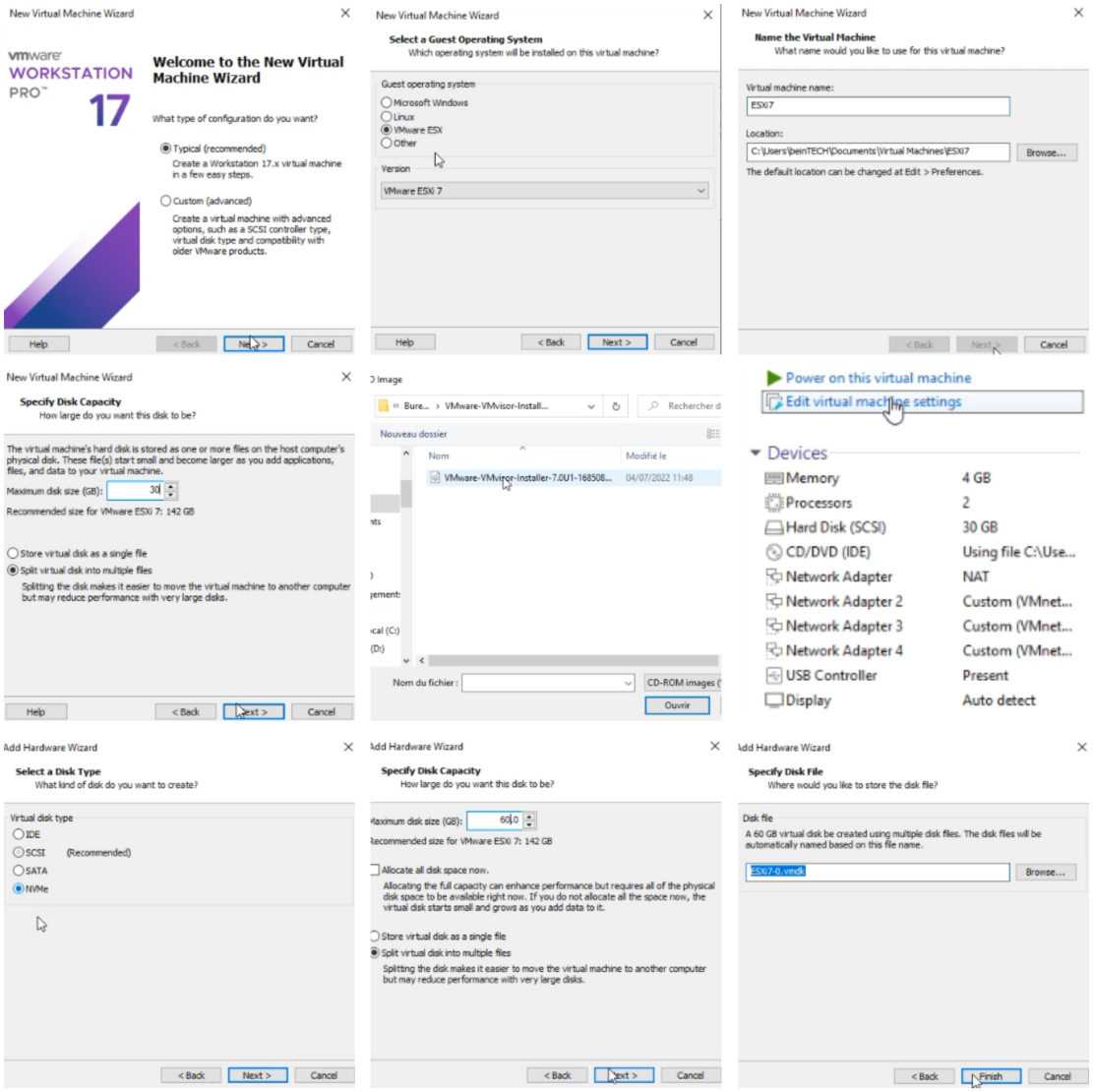


FIGURE 4.96 – Les étapes de L'ajout d'une nouvelle machine virtuelle

2. Nous avons cliqué sur "Power on this virtual machine" pour lancer l'installation de l'ESXi. Au lancement de la VM, nous avons attendu le chargement de l'installeur ESXi.

FIGURE 4.97 – Lancement de l'installation

3. Nous avons appuyé sur F11 pour accepter la licence, puis sur Entrée pour continuer.

4. Nous avons laissé le disque par défaut et appuyé sur Entrée. En utilisant les flèches de notre clavier, nous avons sélectionné la langue de notre clavier (SwissFrench) et appuyé sur Entrée.

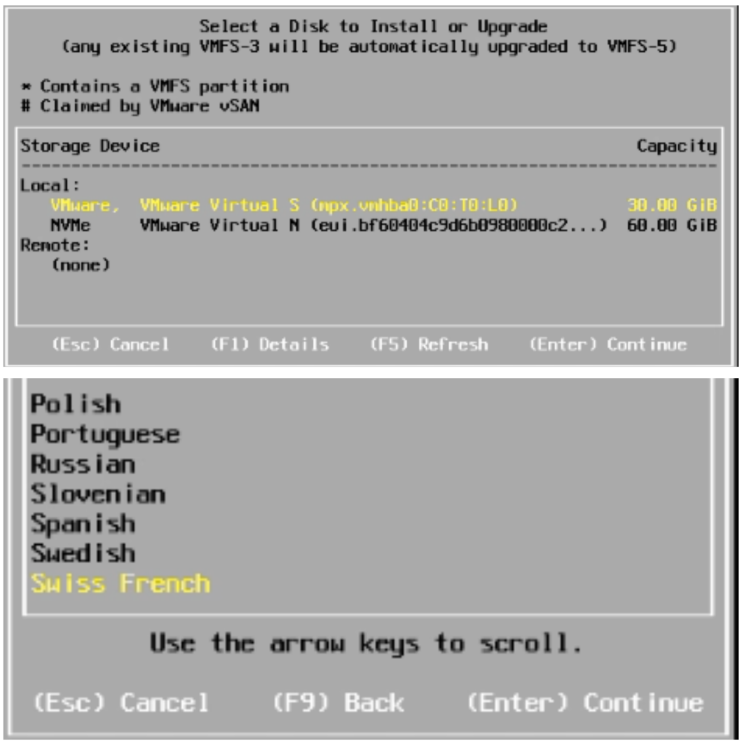


FIGURE 4.98 – Changement de la langue de clavier

5. Nous avons entré un mot de passe pour le compte root, puis nous avons appuyé sur F11 pour lancer l'installation. Une fois celle-ci terminée, nous avons appuyé sur Entrée pour redémarrer.

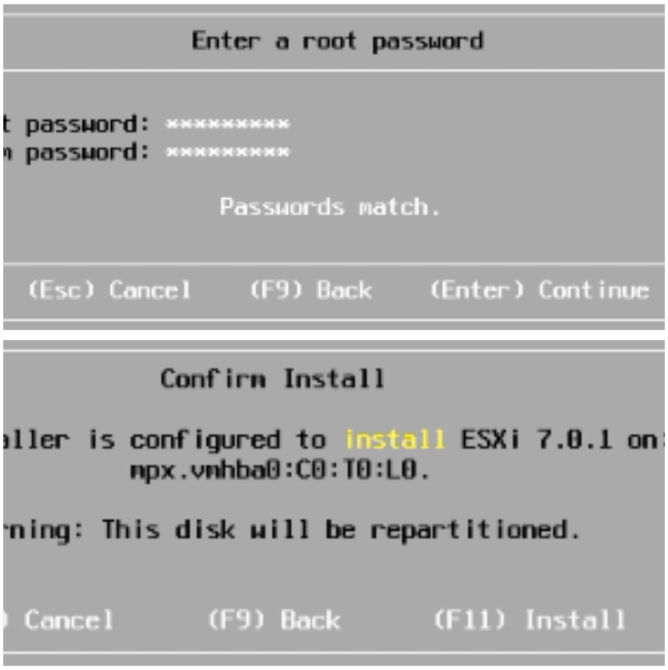


FIGURE 4.99 – Affectation d'un mot de passe pour le compte root

6. L'installation est terminer.

FIGURE 4.100 – La fin de l'installation

4.6.4 Configuration ESXI 7.0

1. Nous nous sommes connectés à l'interface web en ouvrant notre navigateur et en avons entré l'adresse du serveur (par exemple, notre adresse IP : 192.167.131.136).

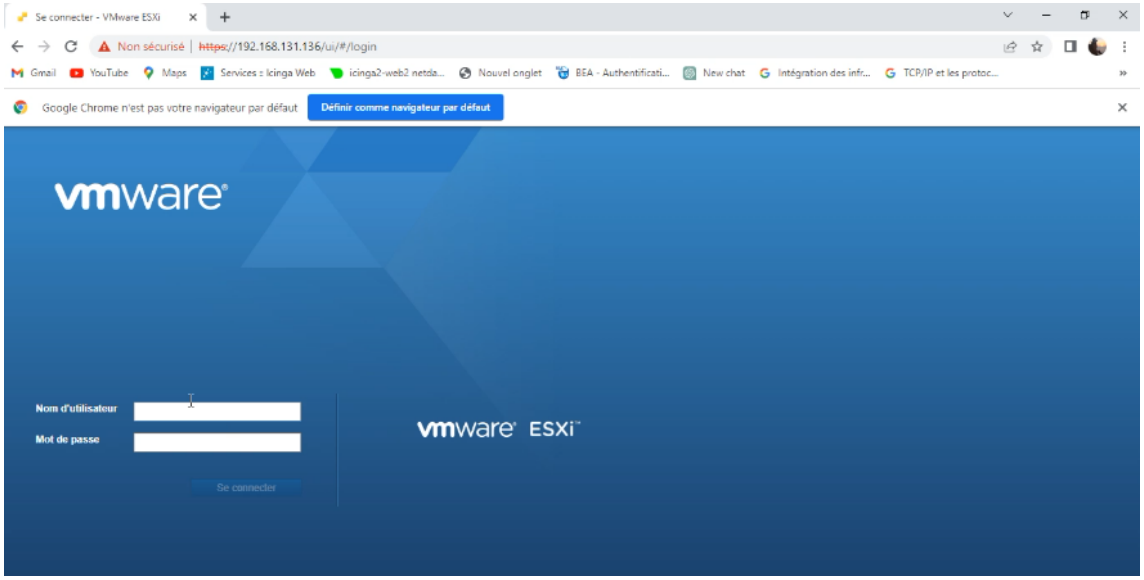


FIGURE 4.101 – Interface d'authentification ESXI 7

2. Nous nous sommes connectés à l'interface web de l'ESXi : https ://esxi-70.pixelabs.lan Nous nous sommes connectés depuis notre contrôleur de domaine : DC-PIXEL01 Login : root Password : votre mot de passe (Asr**2023)

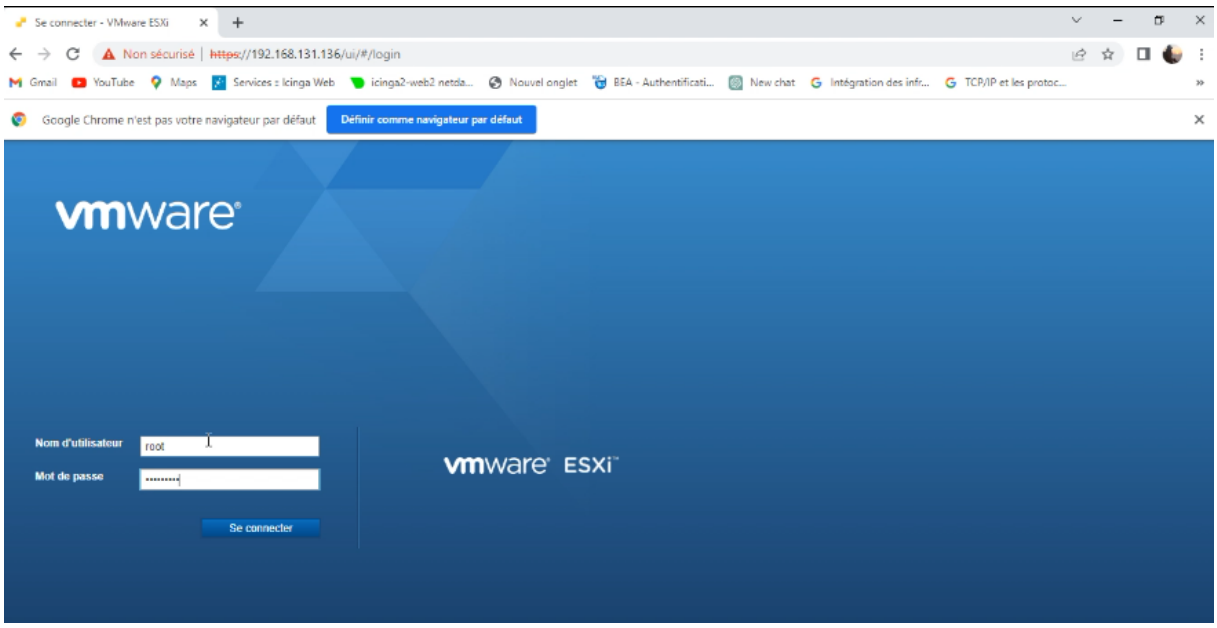


FIGURE 4.102 – Connexion avec le compte root

3. Nous avons créé un nouvel utilisateur Veeam en tant qu'administrateur.

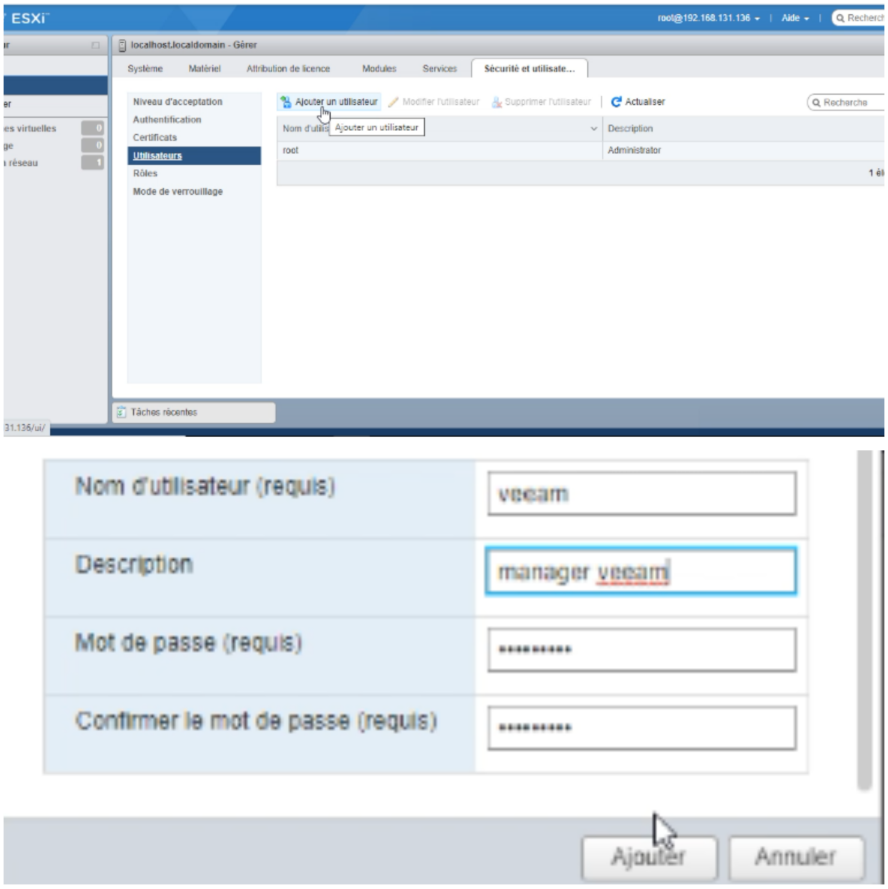
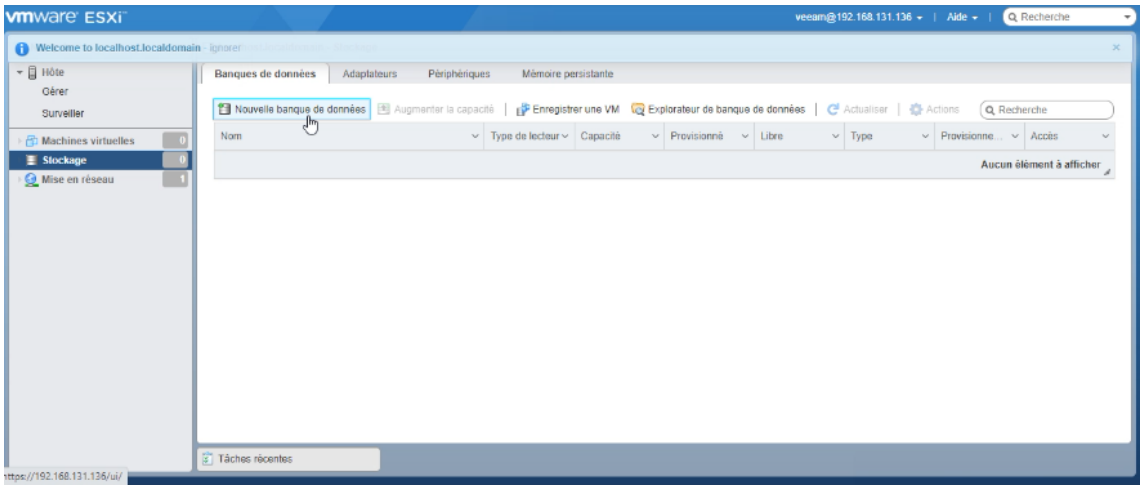


FIGURE 4.103 – Création d'un nouveau utilisateur"veeam"

4. Creation de la base de donnée

   (a) Depuis l'interface web de votre serveur ESXi 7, nous sommes allés dans le menu Stockage > Banque de données (Datastore).

   Nous avons cliqué sur Nouvelle banque de données.



   (b) Nous avons donné un nom à notre datastore et sélectionné notre disque en bas, Ensuite, nous avons cliqué sur Suivant.

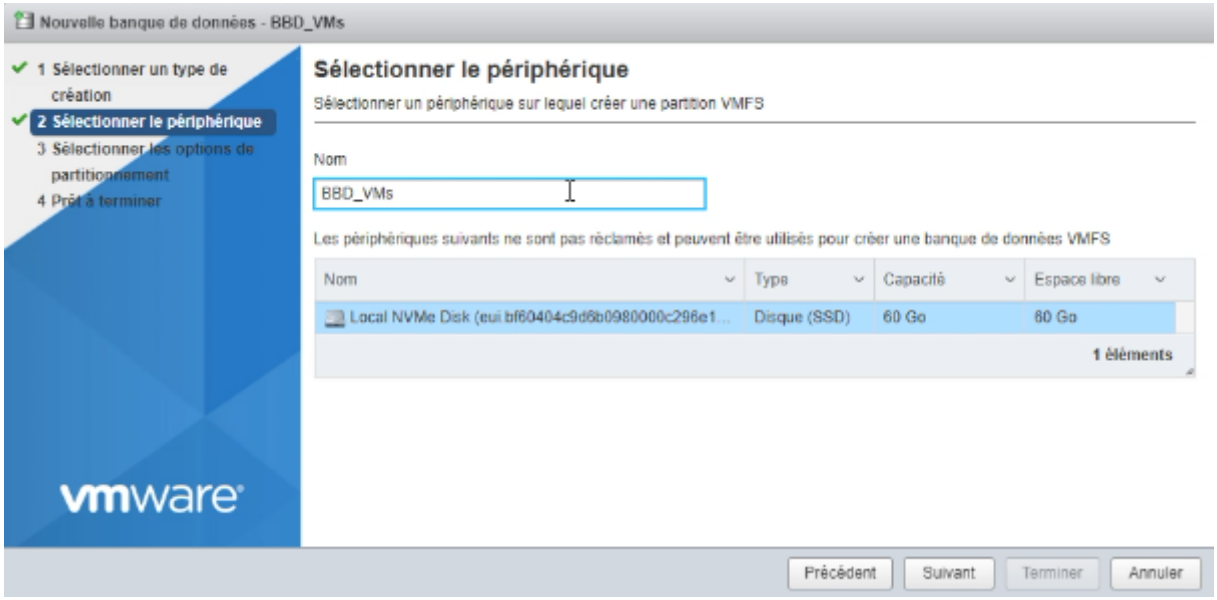


FIGURE 4.104 – Nommer la base de donnée

   (c) Cliquez sur Terminer et confirmez en cliquant sur Oui.

5. Nous avons ajouté une nouvelle machine virtuelle Windows Server, en suivant les étapes dans la figure ci-dessus.

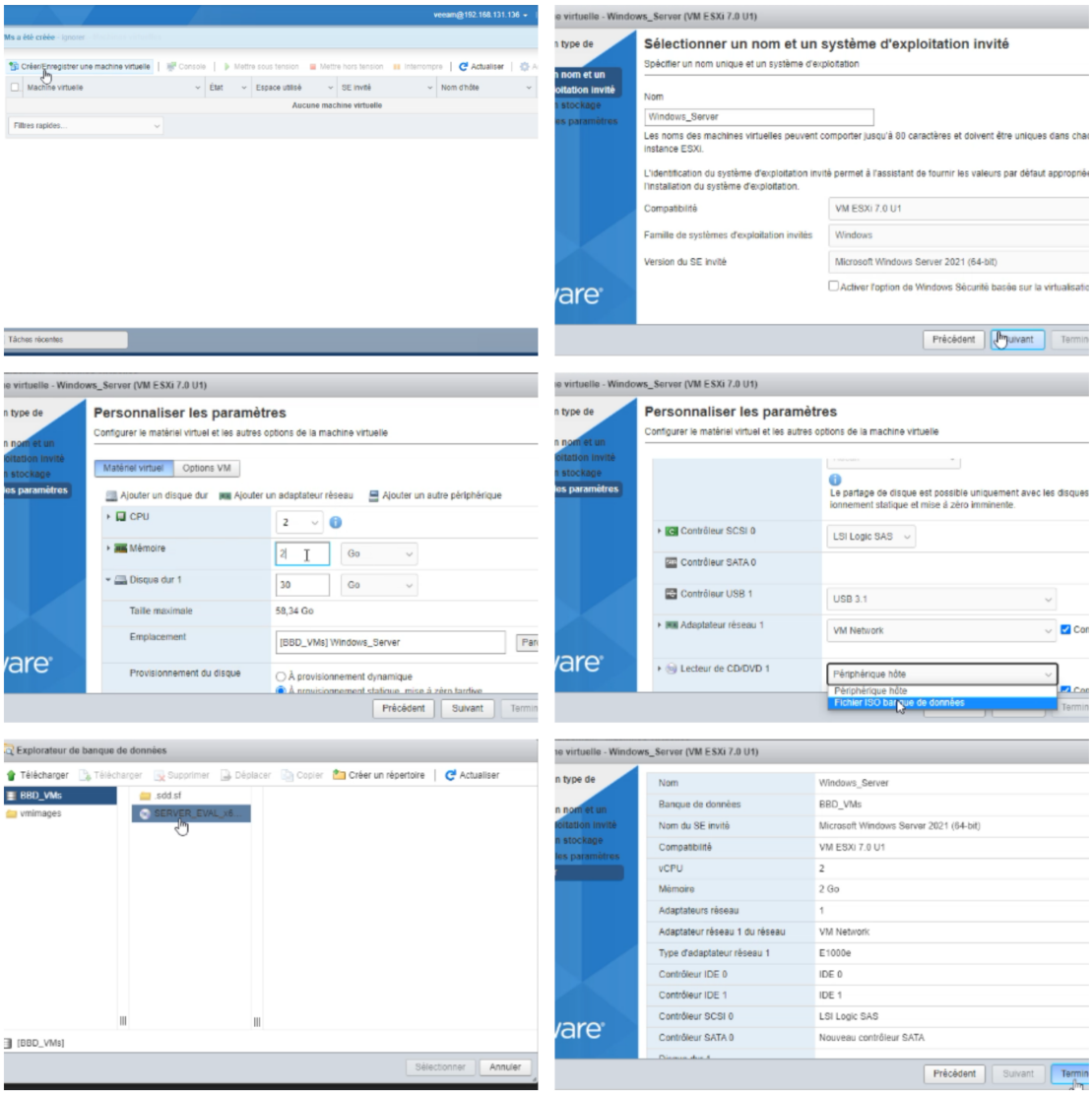


FIGURE 4.105 – L'ajout de la machine vertuelle "Windows_server"

6. Nous avons lancé l'installation de Windows Server et suivi les étapes dans la figure ci-dessus.

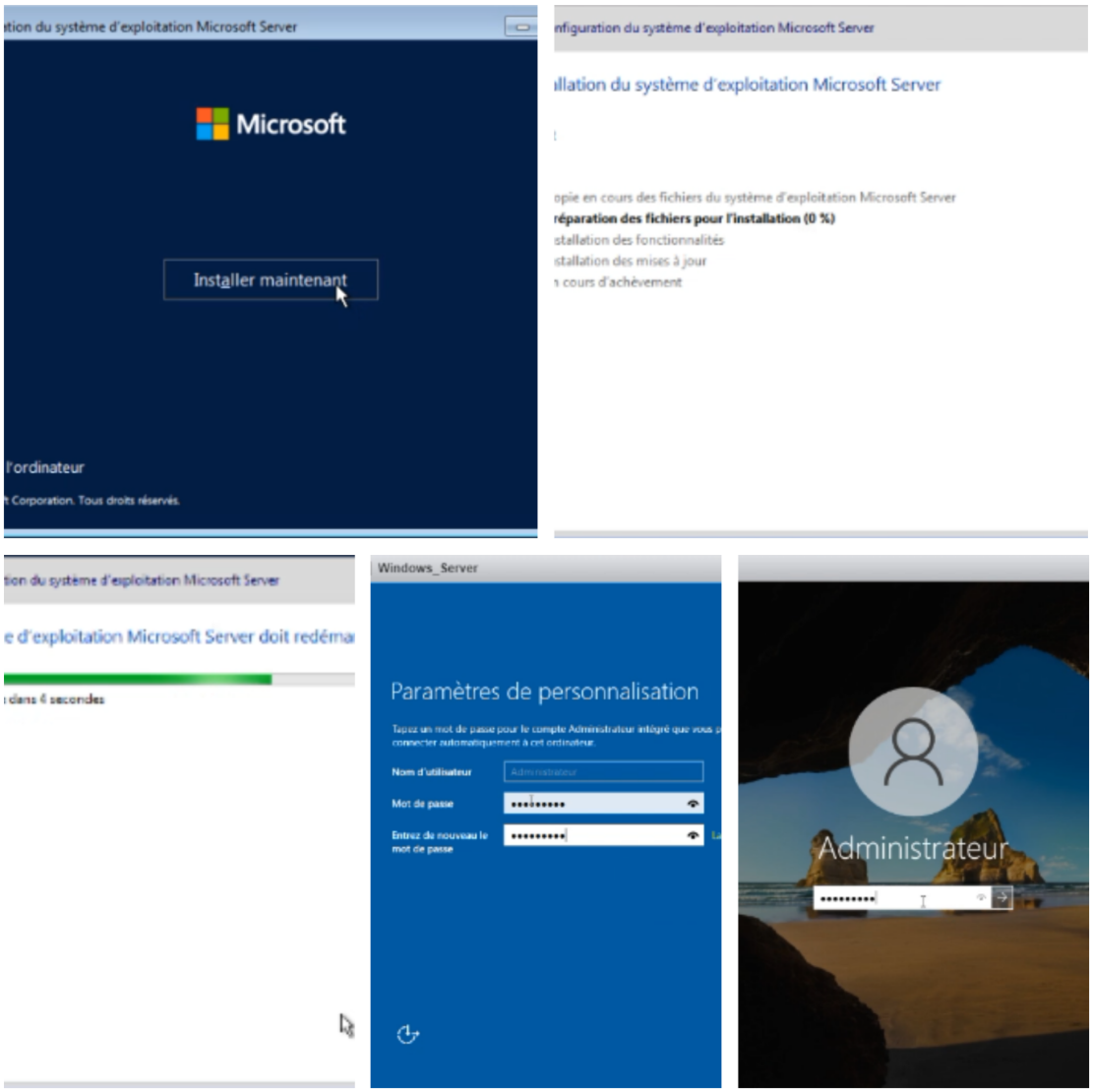


FIGURE 4.106 – Installation "Windows_server"

7. Avec les mêmes étapes , nous avons créé une autre machine virtuelle Linux.

8. Nous avons lancé l'installation de Ubuntu_server et suivi les étapes dans la figure ci-dessus.

FIGURE 4.107 – Installation "Ubuntu_server"

4.6.5 Configuration Veeam Backup & Replication

1. Nous avons ouvert la console "Veeam Backup & Replication" et nous nous sommes connectés à notre serveur de sauvegarde.

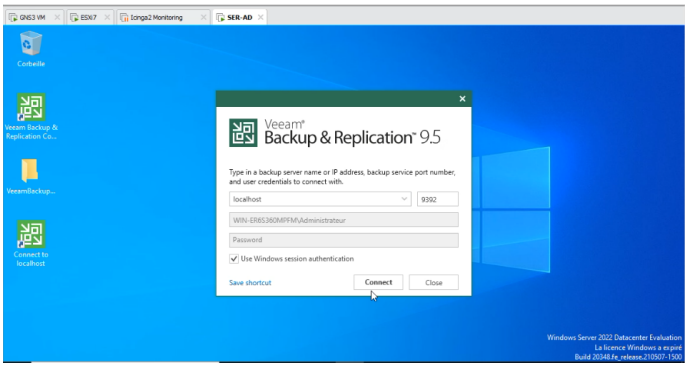


FIGURE 4.108 – L'ouverture de la console "Veeam Backup & Replication"

2. Nous avons ajouter un nouveau disque et nous l'avons nommer "Data_veeam", comme illustré dans la figure ci-dessus.

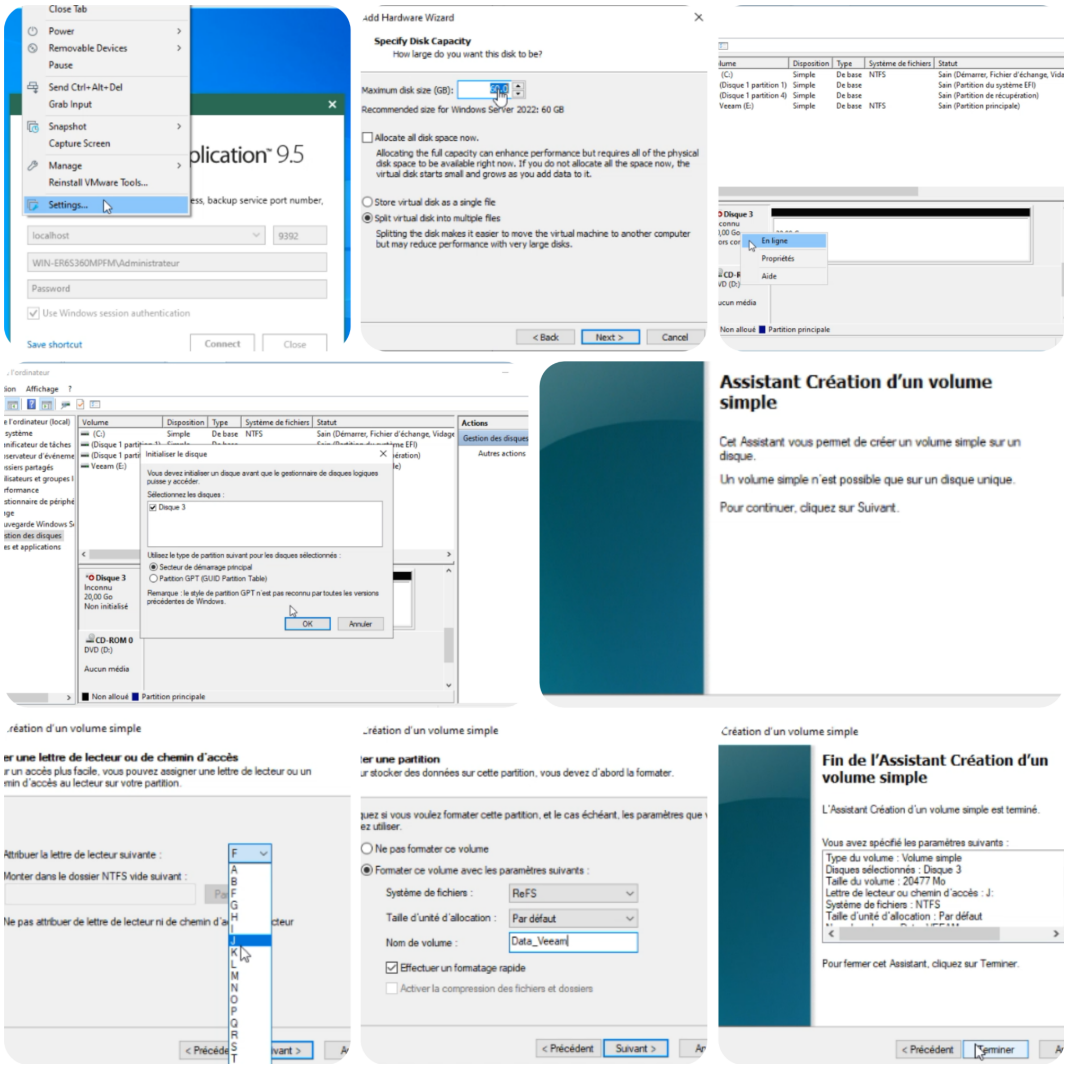


FIGURE 4.109 – Ajout d'un nouveau disk "Data_veeam"

3. Nous avons Ajouté un nouveau disque attaché et nous l'avons nommé "Data Veeam Backup", comme illustré dans la figure ci-dessus.

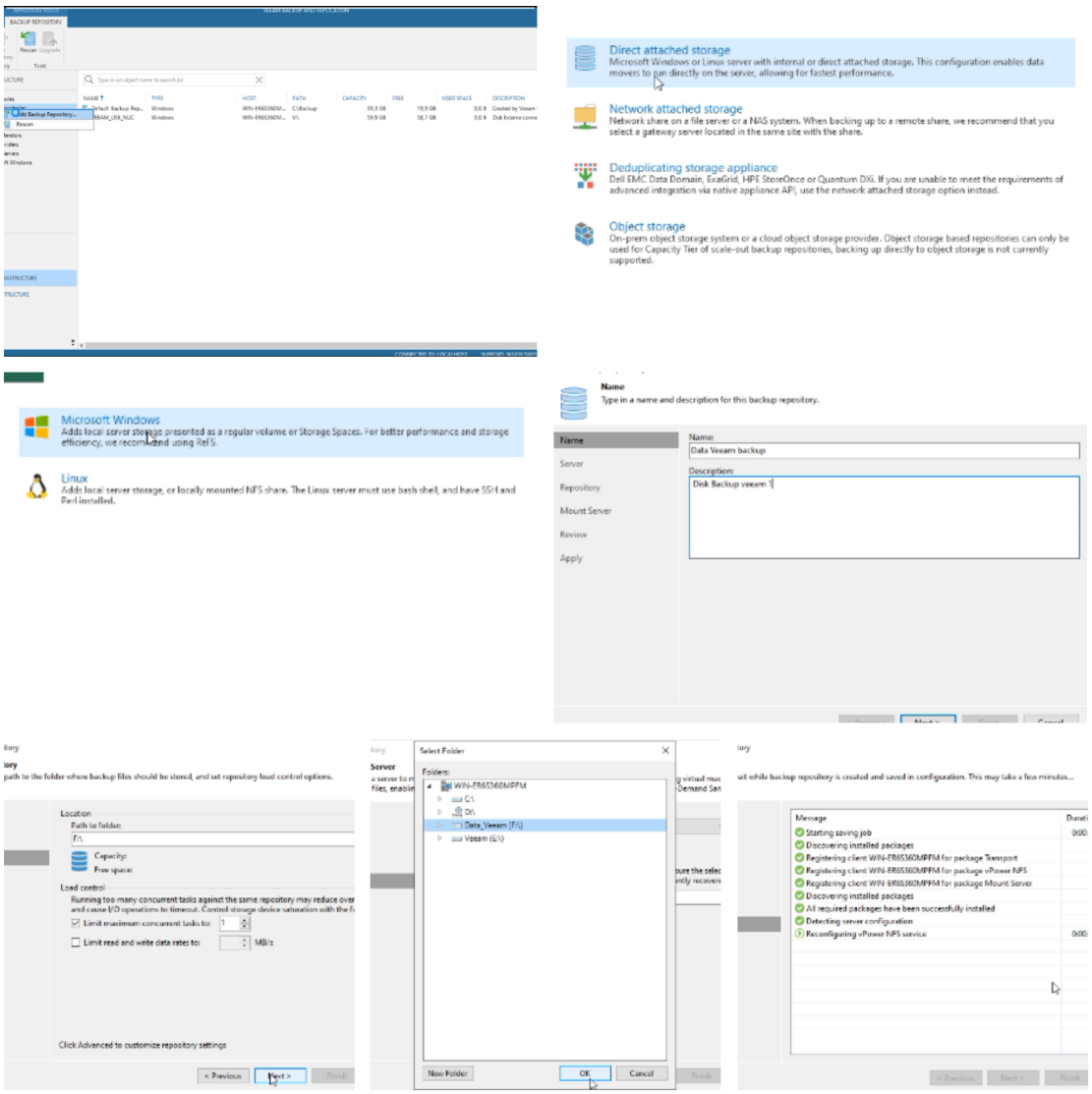


FIGURE 4.110 – Ajout d'un nouveau disk "Data Veeam Backup"

4. Nous avons essayé de nous connecter à notre serveur vSphere en tentant d'abord de faire un ping vers notre serveur.

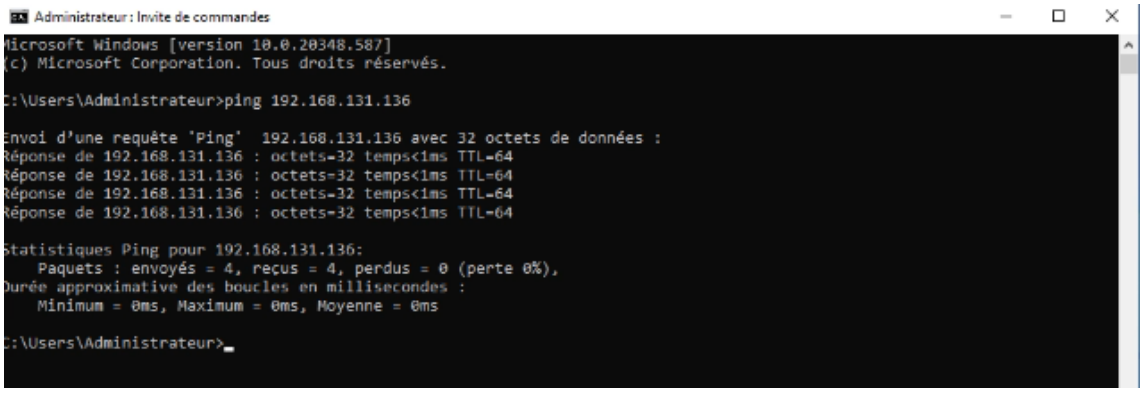


FIGURE 4.111 – Résultat de ping vers notre serveur

5. Nous nous sommes dirigés vers la section "Managed servers" et avons cliqué sur "Add server" pour commencer le processus d'ajout de notre serveur.

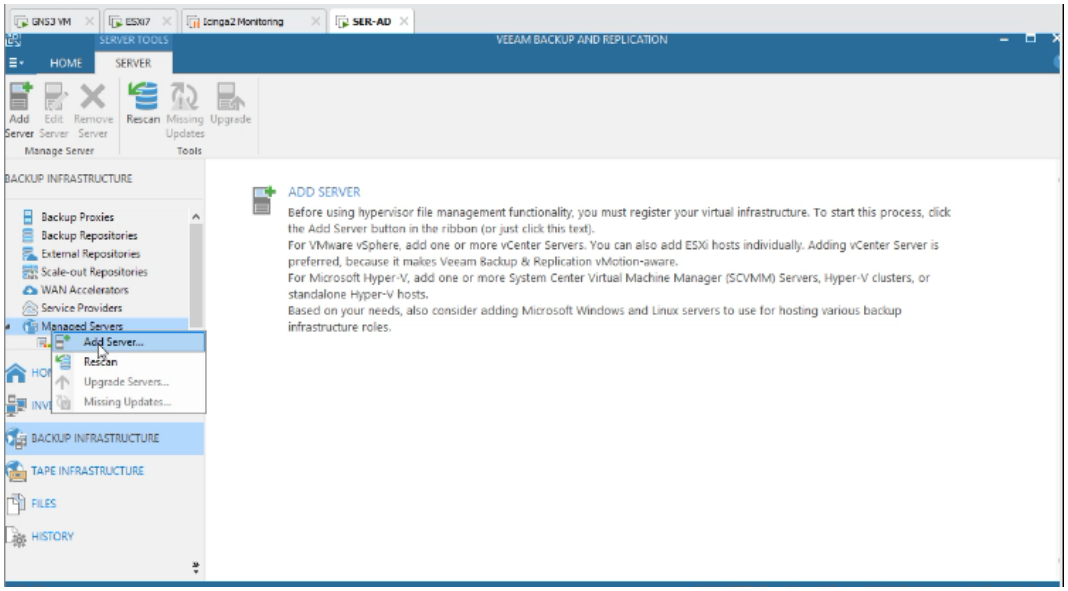


FIGURE 4.112 – Add server

6. Notre serveur est dans la plateforme VMware.

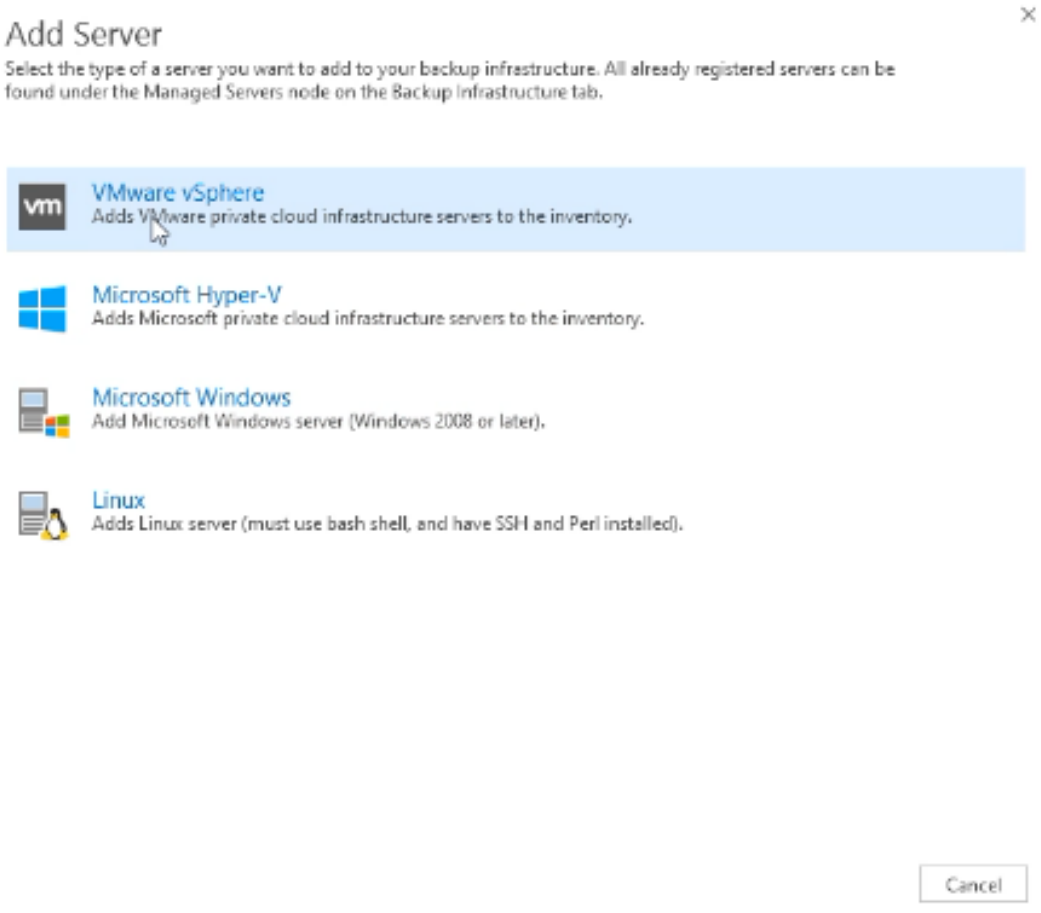


FIGURE 4.113 – Platforme de serveur

7. Nous avons entré l'adresse de notre serveur dans le champ approprié.

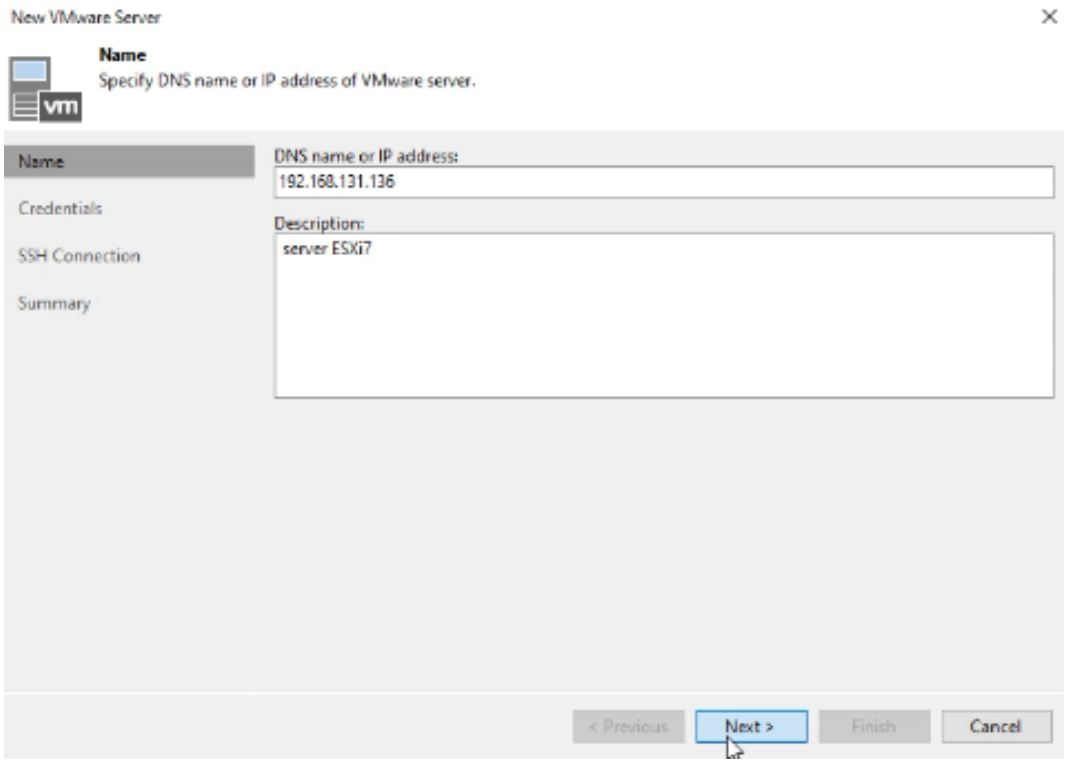


FIGURE 4.114 – La saisie de l'adresse de notre serveur

8. Nous avons saisi les informations de notre compte Veeam déjà créé dans les champs correspondants.

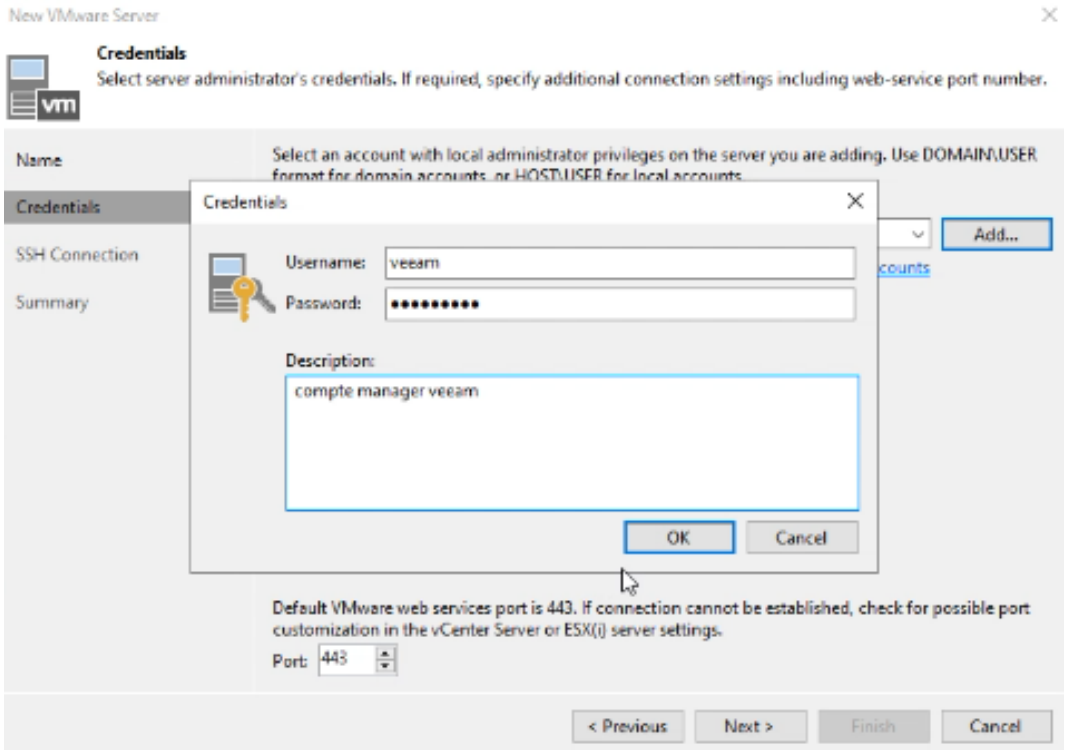


FIGURE 4.115 – La saisie de les informations de notre compte Veeam

9. Une fois cette fenêtre affichée, cela signifie que la connexion a été établie avec succès. Nous avons cliqué sur "Finish" pour finaliser le processus.

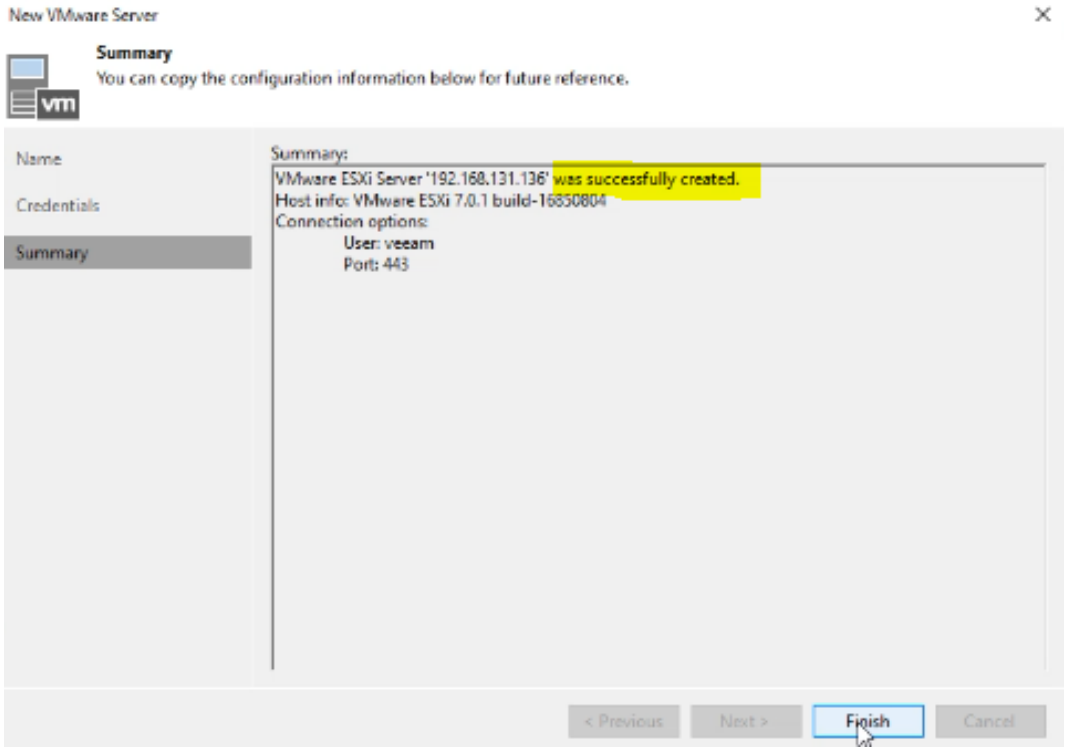


FIGURE 4.116 – la connexion a été établie avec succès

4.6.6 La sauvegarde pour les serveurs Windows et Linux

La sauvegarde du serveur windows "Windows_server"

Pour effectuer une sauvegarde de notre serveur Windows, nous avons suivi les étapes suivantes

1. Dans le menu principal, nous avons sélectionné l'option de sauvegarde "Jobs _> Backup _> Virtuel Machine

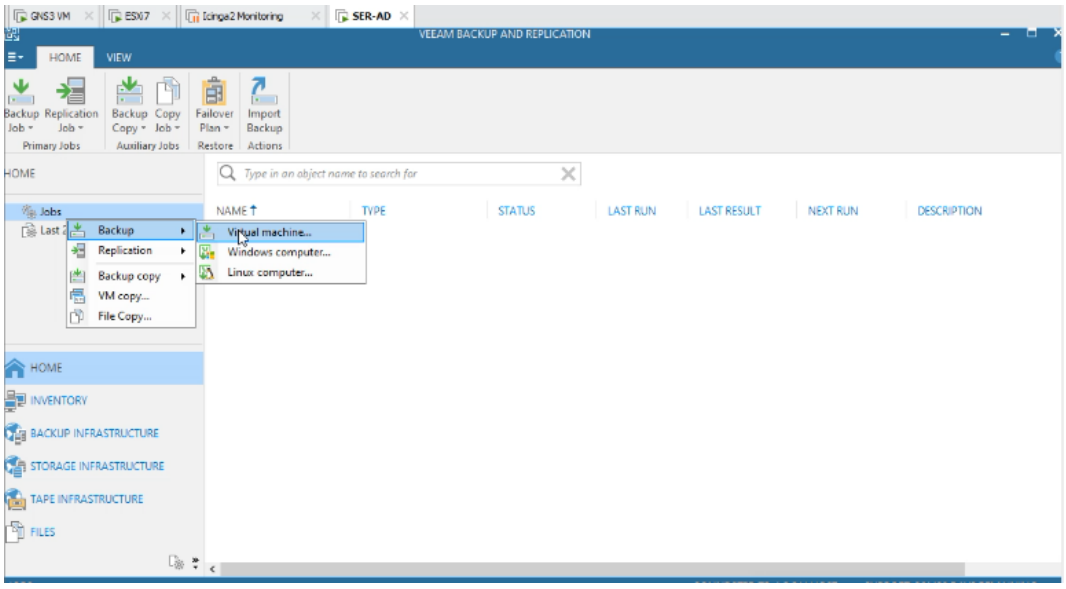


FIGURE 4.117 – La sélection de l'option de sauvegarde

2. Nous avons renommé notre Jobs.

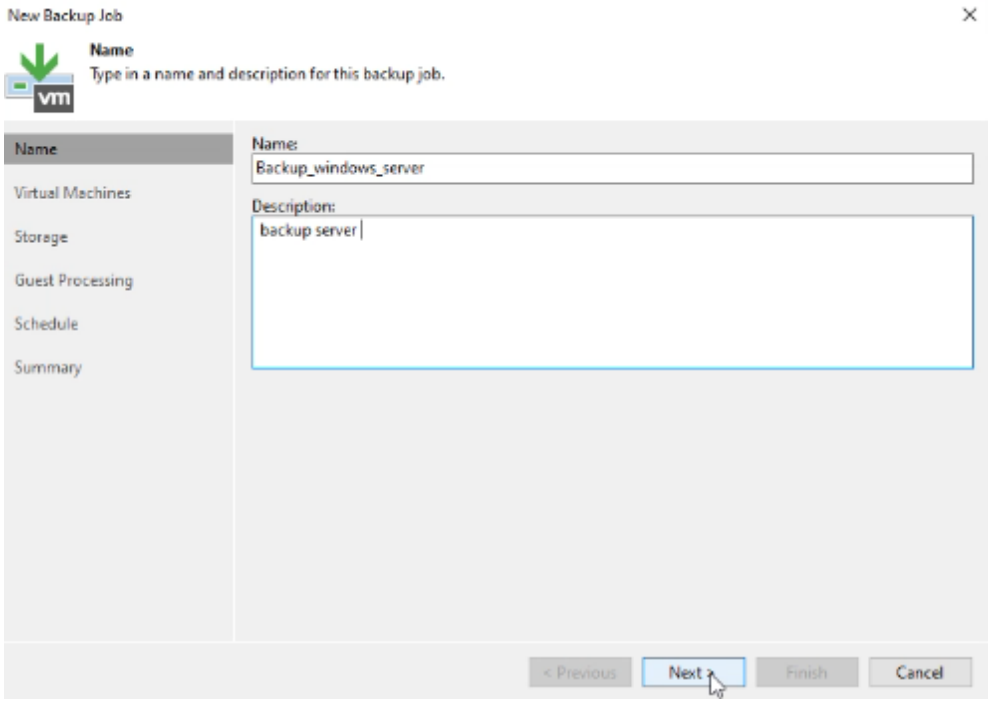


FIGURE 4.118 – Renommé notre Jobs

3. Nous avons choisi notre serveur Windows dans la liste des sources de sauvegarde.

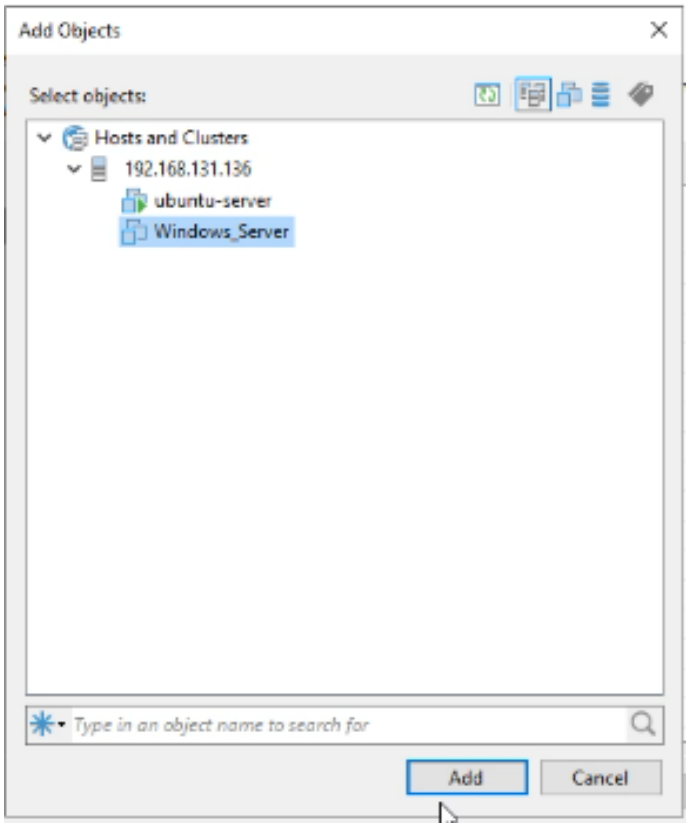


FIGURE 4.119 – choisi notre serveur Windows

4. Après nous allons choisir le disque où nous avons sauvegardé.

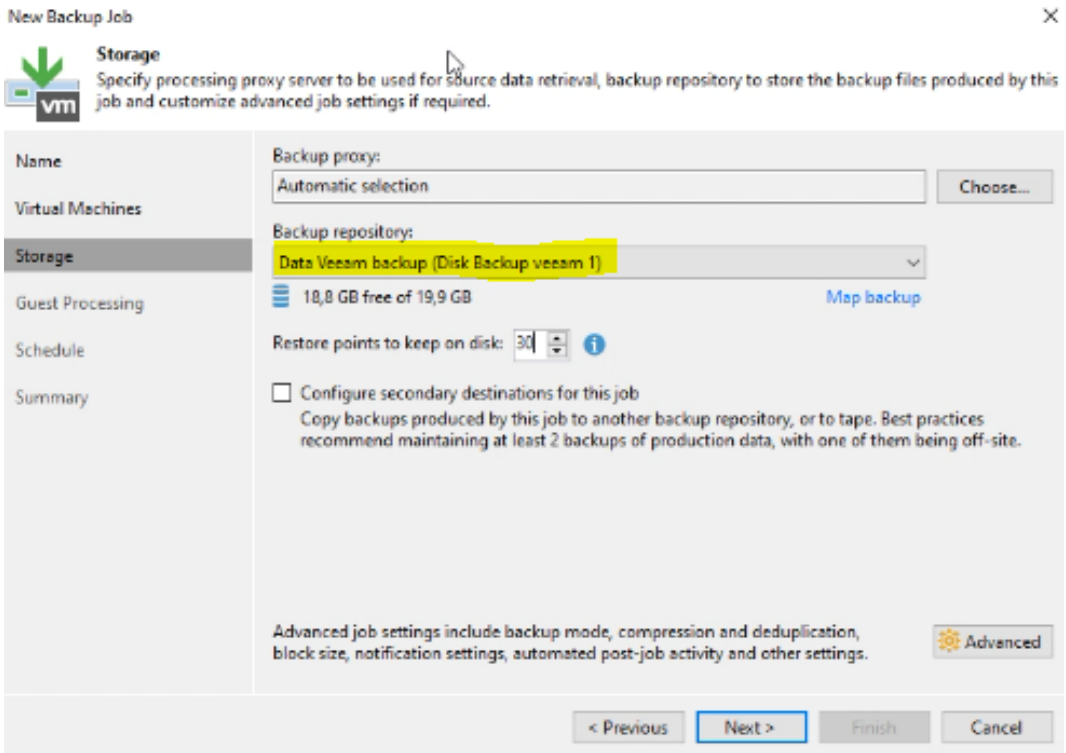


FIGURE 4.120 – choisir le disque

5. Ensuite, nous avons configuré les paramètres de sauvegarde . On a cliqué sur "Apply" puis sur "Finish" .

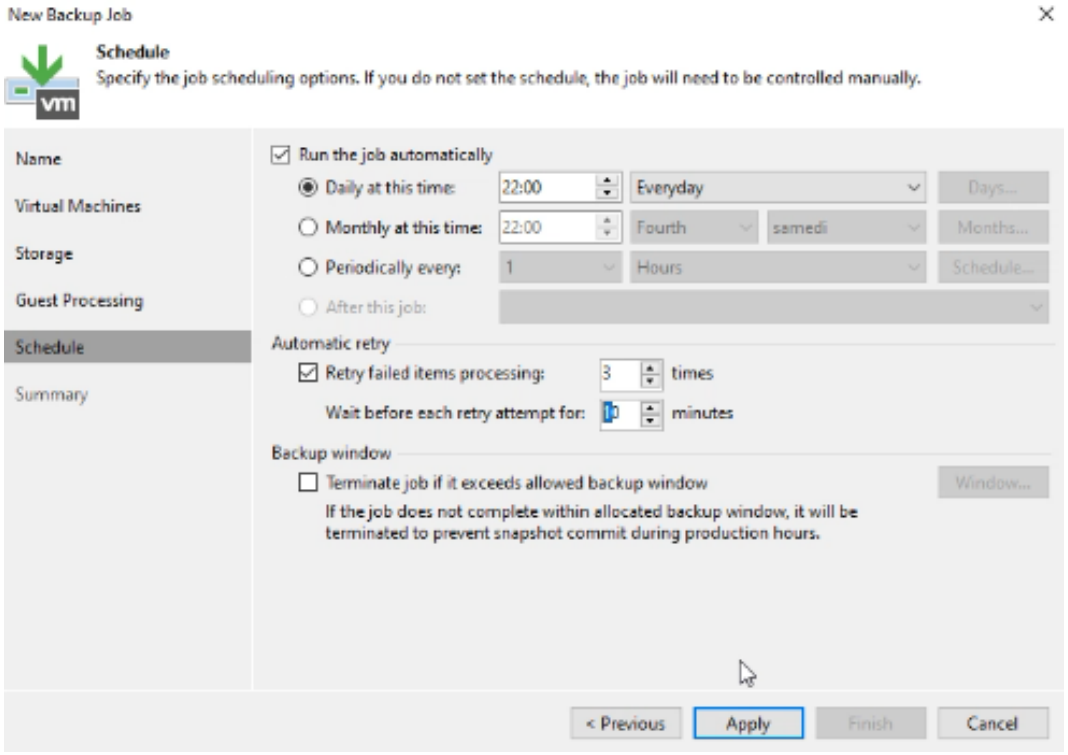


Figure 4.121 – La sauvegarde est terminer

La sauvegarde du serveur ubuntu "Ubuntu_server

Nous avons suivi les étapes précédentes de manière similaire pour effectuer la sauvegarde de notre serveur Ubuntu.

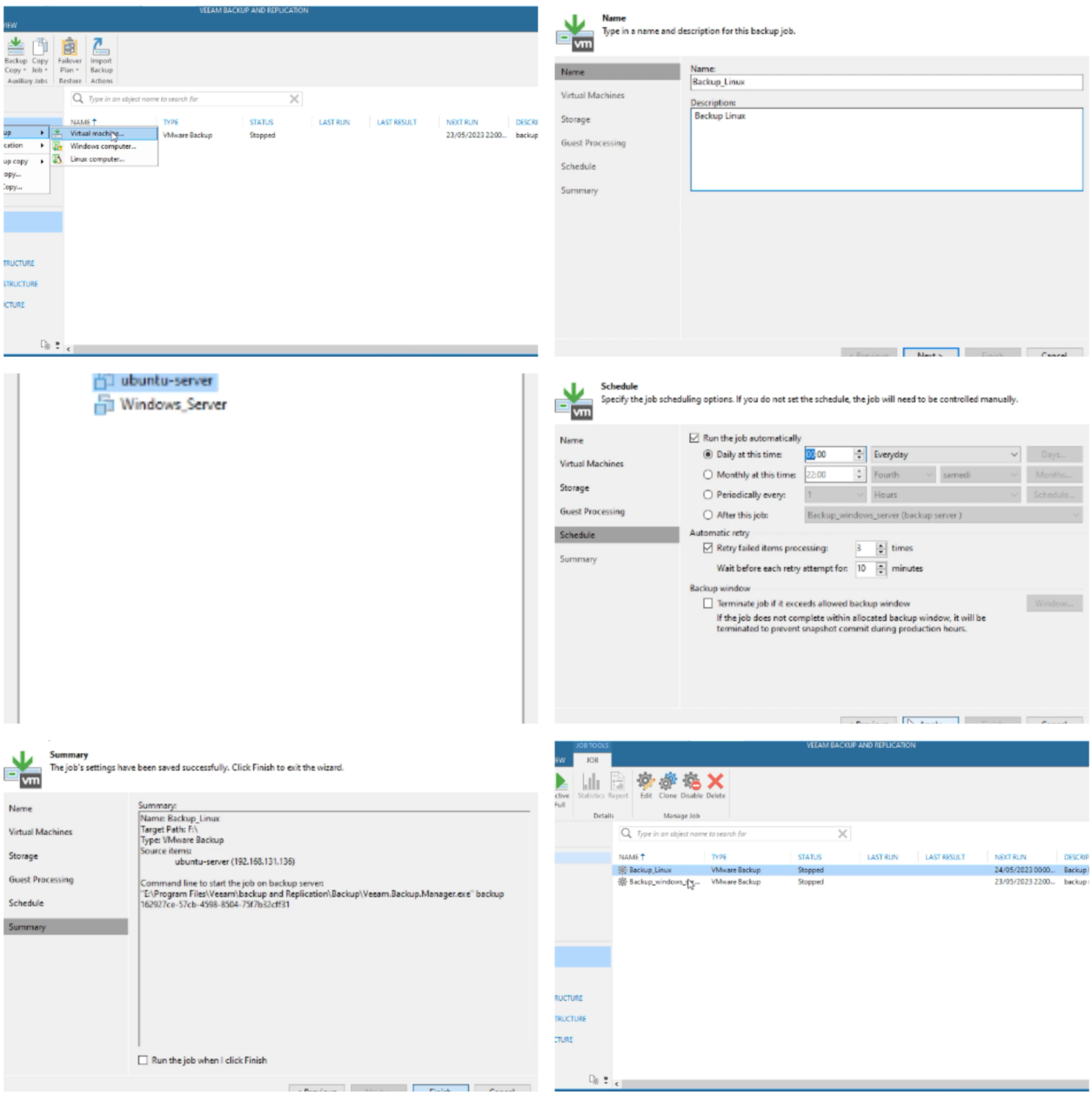


FIGURE 4.122 – La sauvegarde est terminer

4.6.7 La réplication pour le serveur Ubuntu

Pour effectuer une réplication de notre serveur ubuntu, nous avons suivi les étapes suivantes :

1. Dans le menu principal, nous avons sélectionné l'option de sauvegarde "Jobs _> Backup _> Virtuel Machine

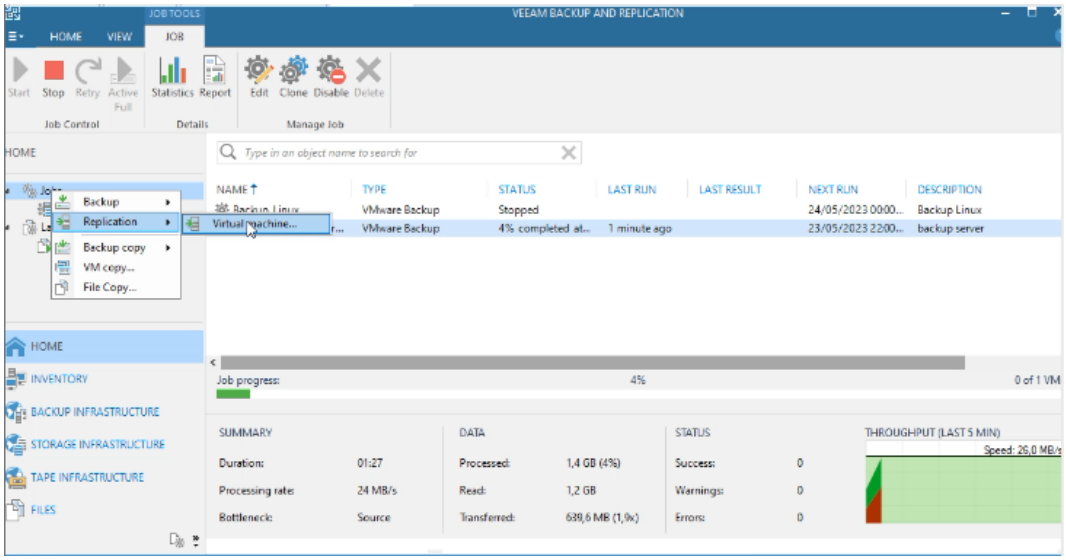


FIGURE 4.123 – La sélection de l'option de réplication

2. Nous avons renommé notre Jobs.

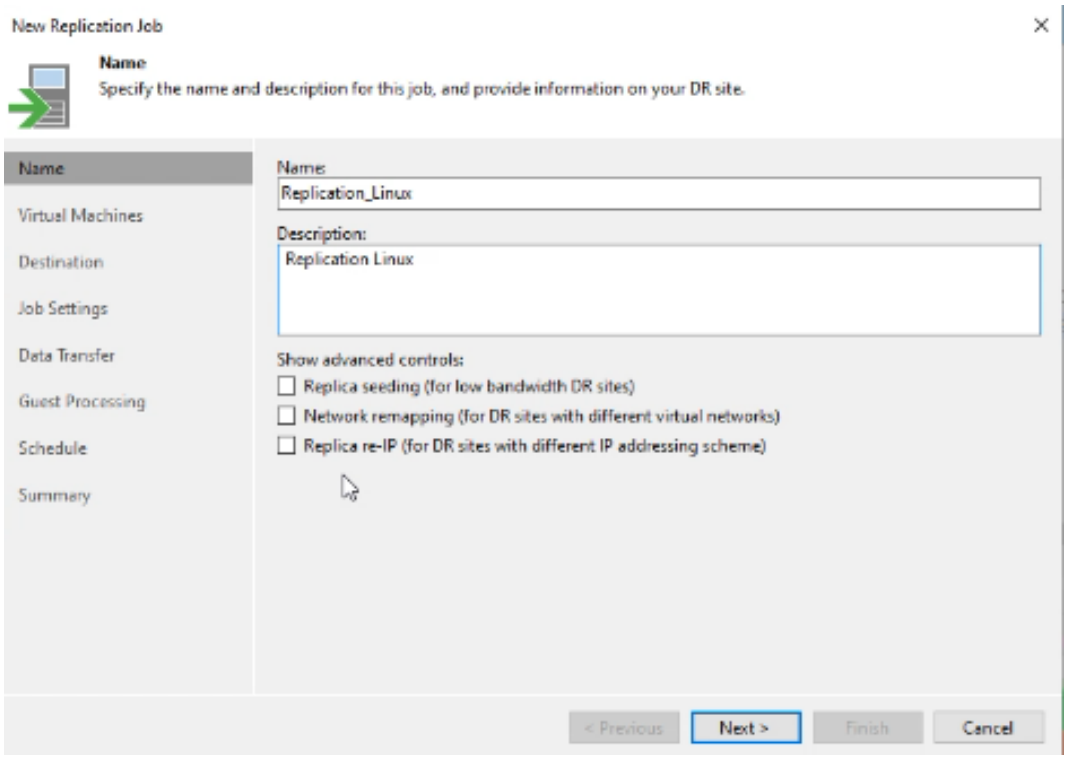


FIGURE 4.124 – Renommé notre Jobs

3. Nous avons choisi notre serveur Ubuntu .

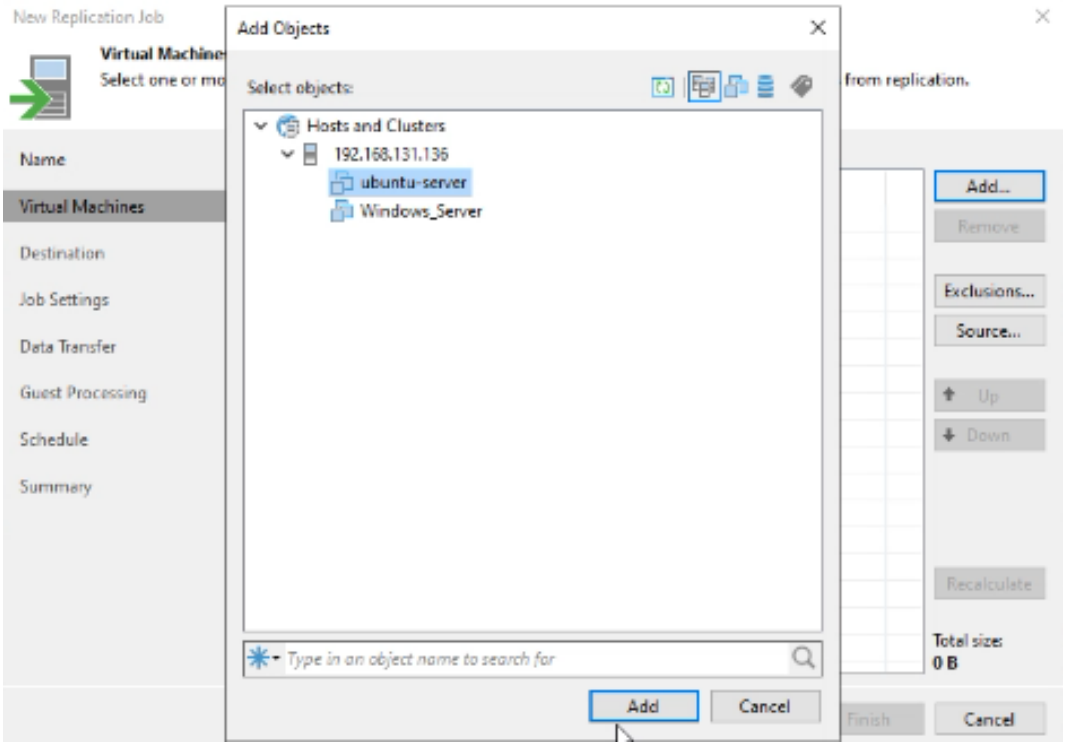


FIGURE 4.125 – choisi notre serveur Ubuntu

4. Ensuite,Nous avons entré l'adresse de notre serveur dans le champ approprié.

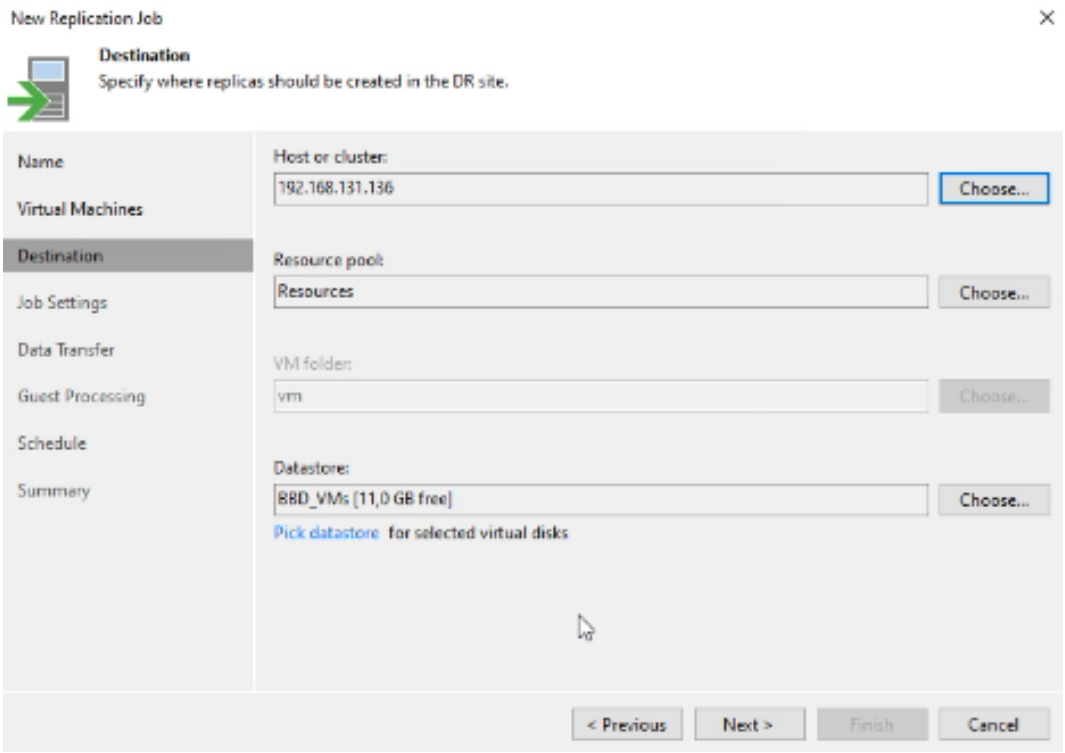


FIGURE 4.126 – La saisie de l'adresse de notre serveur

5. Enfin, nous avons configuré les paramètres de sauvegarde . On a cliqué sur "Apply" puis sur "Finish"

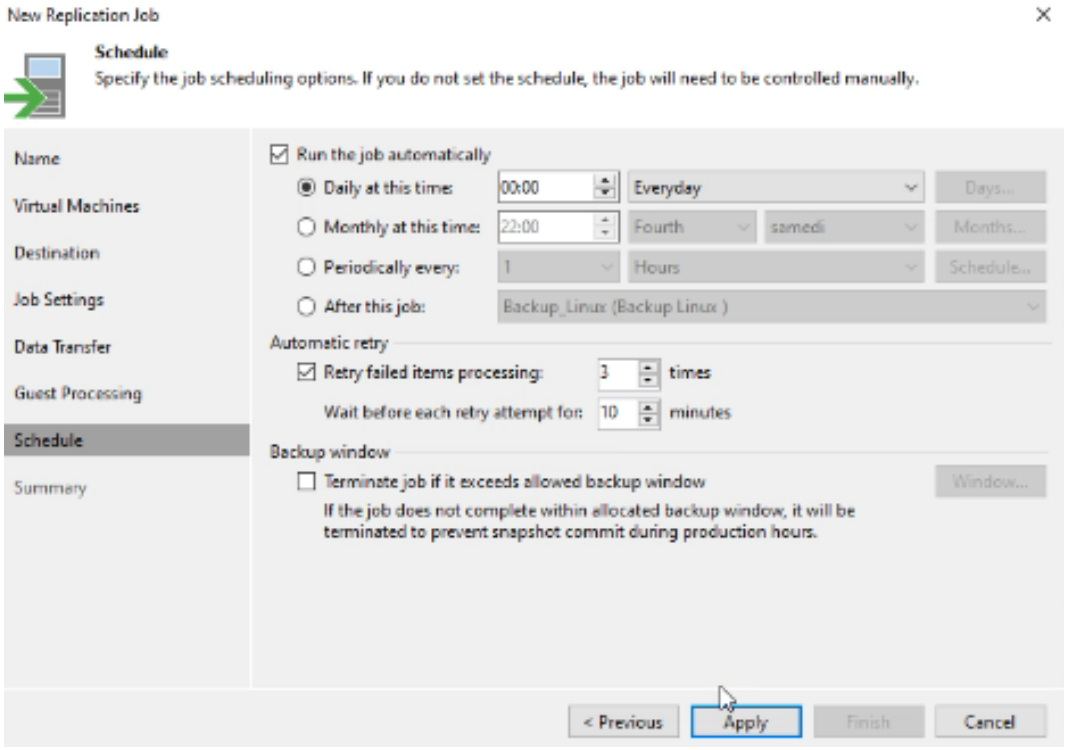


FIGURE 4.127 – La réplication est terminer

4.6.8 Test

1. Nous avons cliqué sur "Start" pour lancer le processus de sauvegarde pour notre serveur Windows.

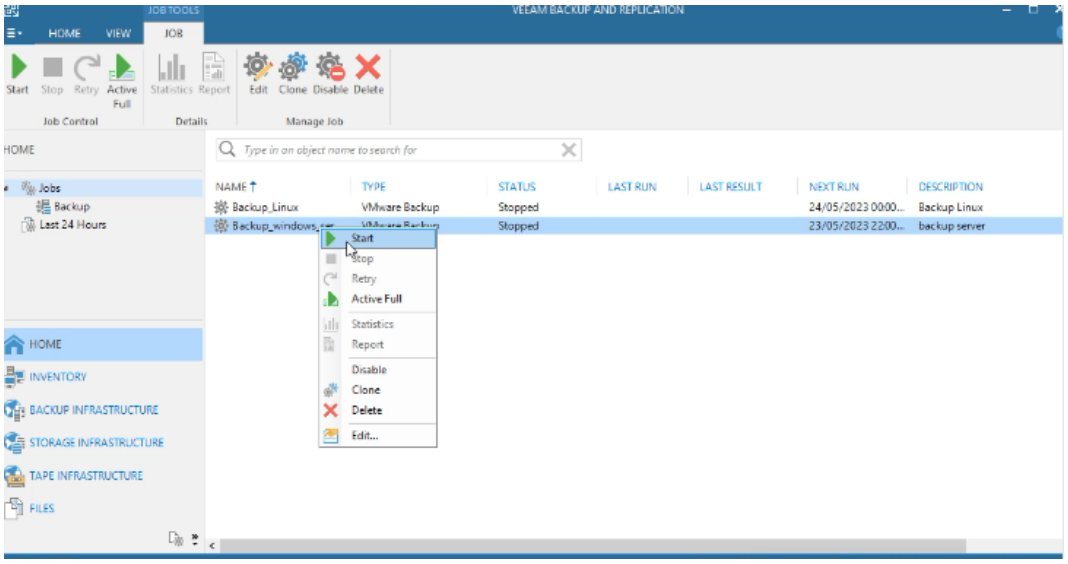


FIGURE 4.128 – Lancement de la sauvegarde

2. Notre sauvegarde a été effectuée avec succès"

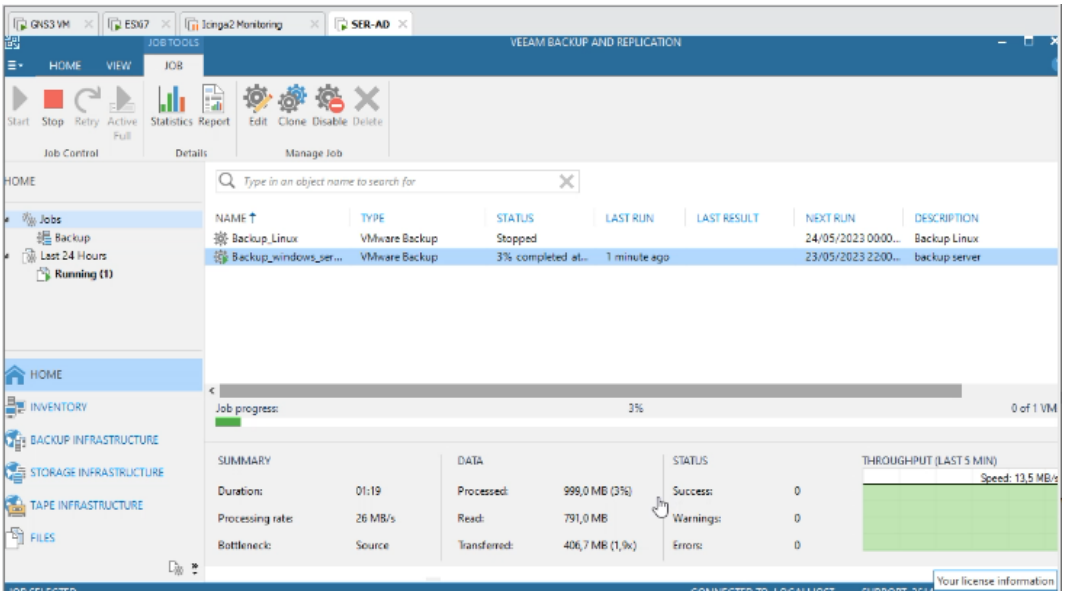


FIGURE 4.129 – La sauvegarde a été effectuée avec succès

Conclusion

Dans ce chapitre, nous avons présente les éléments clés de notre partie pratique. Ou nous avons décrire les étapes d'installation et de configuration de déférentes processus suivi, Par la suite, nous avons produis quelque résultat de cette solution de supervision.

Conclusion générale

Notre objectif principal était de mettre en place une console d'administration réseau au sein de l'entreprise Cevital Bejaia. Pour commencer, nous avons présenté l'organisme d'accueil CEVITAL de Béjaia, en mettant en évidence sa création, son évolution, sa situation géographique et son organigramme général. Nous avons réalisé une étude de l'existant en examinant l'infrastructure de l'entreprise, l'architecture globale de son réseau, le matériel et le logiciel utilisés, ainsi que l'analyse du parc informatique.

Ensuite, nous avons exposé la problématique identifiée et proposé une solution pour y faire face. Nous avons décrit le contexte du projet, y compris le projet lui-même, le cahier des charges et l'analyse des besoins.

Nous avons abordé les notions de base sur les systèmes d'exploitation et les réseaux informatiques, en fournissant des définitions, des objectifs, des classifications, des architectures, des topologies, des normes de communication et des protocoles réseau.

Dans notre projet, nous avons également traité de la supervision, de la sauvegarde et de la réplication informatique. Nous avons expliqué la supervision comme le suivi et le contrôle des équipements, en présentant le protocole SNMP. Nous avons abordé la sauvegarde, qui consiste à préserver les données importantes, en décrivant ses principes et ses types. Nous avons présenté la réplication, qui vise à créer des copies de données, avec ses objectifs et ses mécanismes.

Enfin, nous avons exposé la réalisation et les tests, en détaillant l'environnement de travail, l'architecture proposée et la configuration des équipements. Nous avons suivi une méthodologie pour effectuer les différentes étapes, telles que la configuration des interfaces, la création des VLANs, l'affectation des ports, la configuration du pare-feu et des routeurs.

Notre mémoire nous a permis de mieux comprendre l'entreprise CEVITAL de Béjaia, son infrastructure informatique et les enjeux liés à la supervision, à la sauvegarde et à la réplication. Les solutions que nous avons proposées peuvent contribuer à améliorer la gestion et la sécurité des systèmes informatiques de l'entreprise.

En conclusion, notre projet a approfondi nos connaissances sur l'entreprise CEVITAL, l'analyse de son infrastructure informatique, ainsi que sur les systèmes d'exploitation, les réseaux informatiques, la supervision, la sauvegarde et la réplication. Il constitue une base solide pour toute personne intéressée par ces domaines et peut servir de référence pour d'autres projets similaires.

Bibliographie

[1] Atelin, P. *Réseaux informatiques : notions fondamentales : normes, architecture, modèles OSI, TCP/IP, Ethernet, Wi-Fi,...* Editions ENI, 2009.

[2] Atelin, P., and Dordoigne, J. *TCP/IP et les protocoles Internet.* Editions ENI, 2006.

[3] BELKHOUCHE, S. Etude et administration des systèmes de supervision dans un réseau local.

[4] Case, J., Fedor, M., Schoffstall, M., and Davin, J. Rfc1098 : Simple network management protocol (snmp), 1989.

[5] Cougias, D. J., Heiberger, E. L., and Koop, K. *The backup book : disaster recovery from desktop to data center.* Network Frontiers, 2003.

[6] De Guise, P. *Data protection : Ensuring data availability.* CRC Press, 2020.

[7] Decan, A. *Système de backup distribué.* PhD thesis, Master's thesis, Université de Mons-Hainaut, 2007.

[8] Dromard, D., and Seret, D. *Architecture des réseaux.* Pearson Education France, 2013.

[9] Fassino, J.-P. *THINK : vers une architecture de systèmes flexibles.* PhD thesis, Télécom ParisTech, 2001.

[10] Festor, O. *Formalisation du comportement des objets gérés dans le cadre du modèle OSI.* PhD thesis, Université Henri Poincaré-Nancy 1, 1994.

[11] Gauthier, L. *Génération de système d'exploitation pour le ciblage de logiciel multitâche sur des architectures multiprocesseurs hétérogènes dans le cadre des systèmes embarqués spécifiques.* PhD thesis, Institut National Polytechnique de Grenoble-INPG, 2001.

[12] Ghezal, A., and Chimi, K. *IoT Monitoring : État de l'art des solutions existantes.* PhD thesis, Université Ibn Khaldoun-Tiaret-, 2019.

[13] Kadoch, M. *Protocoles et réseaux locaux : 2e édition revue et augmentée.* PUQ, 2012.

[14] MarcNAKANNABO, M., Sadouanouan, M., SOUABO, O., and TRAORE, A. K. Du reseau informatique du siege de la sofitex.

[15] Megzari, P. O. SystÈmes d'exploitation.

[16] Mohamed, G., and Amine, R. La mise en place et la gestion d'un réseau informatique au sein de la fsei.

[17] Mourlhon-Dallies, F., and Colin, J.-Y. Les rituels énonciatifs des réseaux informatiques entre scientifiques. *Les Carnets du Cediscor. Publication du Centre de recherches sur la didactique des discours ordinaires*, 3 (1995), 161–172.

[18] Mérè, A. La gestion réseau et le protocole snmp. *FIFO04*.

[19] Nussbaum, L., and Richard, O. Prototype de canal caché dans le dns. In *Colloque Francophone sur l'Ingénierie des Protocoles (CFIP), Les Arcs, France* (2008), vol. 3.

[20] Passard, P., and vers IPv, I. Les réseaux informatiques.

[21] Preston, W. C. *Backup and Recovery : Inexpensive Backup Solutions for Open Systems.* " O'Reilly Media, Inc.", 2007.

[22] Reichenbach, F. Service snmp de détection de faute pour des systèmes répartis. Tech. rep., 2002.

[23] Toutain, L. *Réseaux locaux et Internet.* Hermès, 2003.

Résumé

Le réseau informatique d'une entreprise rassemble des objets interconnectés pour échanger des données, il est donc considéré comme le cœur de l'entreprise. En effet, il doit toujours être valide pour garantir l'activité, mais cela ne suffit pas, il doit aussi être tout le temps sous surveillance et les données doivent être toujours disponible , car si l'un des composant de ce mémoire tombe en panne ou défaillant ou bien la perte des données d'une manière intentionnelle ou non intentionnelle peut entraîner des conséquences catastrophique sur le niveau organisationnelle et financier . À cette effet, nous examinons deux technologies de réseau informatique les plus importantes, la supervision réseau et système et la sauvegarde et réplication.

Notre projet comprend l'étude et la mise en place d'une solution de supervision et sauvegarde et réplication réseaux et systèmes au sein de l'entreprise cevital qui assure la surveillance en temps réel et proactive de son infrastructure qui est en constante évolution ainsi garantir la disponibilité des données et d'informations pour cela nous avons choisi la solution de supervision centreon qui fait partie des plus grade plus grande solutions fiable comme nous avons opté pour la solution Veeam Backup pour réaliser les sauvegardes et réplication réseaux et systèmes.

Abstract

The computer network of a company brings together interconnected devices to exchange data, making it the core of the company. It must always be valid to ensure business activity, but that is not enough. It also needs constant monitoring, and the data must always be available. If any component of this network fails or if data is lost intentionally or unintentionally, it can have catastrophic consequences on the organizational and financial levels. Therefore, we are examining two crucial technologies for computer networks: network and system monitoring, and backup and replication.

Our project involves studying and implementing a network and system monitoring, backup, and replication solution within the cevital company. This solution ensures real-time and proactive monitoring of the constantly evolving infrastructure, guaranteeing data and information availability. For this purpose, we have chosen the Centreon monitoring solution, which is one of the most reliable and robust solutions. Additionally, we have opted for the VeemBackup solution for network and system backups and replication.