

Rapport E5

Corentin CHAUVEL

Apprenti Technicien Informatique



Du 01/09/2024 au 31/07/26

Tuteur en entreprise : Vincent VEILLEROBE

Entreprise d'accueil : Région Pays De La Loire

Adresse : 1 Rue de la Loire, 44000 Nantes

Tél : 02 28 20 50 00

Formation : BTS SIO - SISR

Etablissement : UIMM - Fab'Academy Nantes - 9 Rue de l'Halbrane, 44340 Bouguenais

Remerciements

Tout d'abord, je tiens à remercier mon tuteur Vincent VEILLEROBE, pour son soutien, sa disponibilité et ses précieux conseils tout au long de c'est 2 ans. Je remercie aussi tout l'équipe du SI qui mon accompagné tout le long de ces deux années et avec qui j'ai pu découvrir plein de nouvelles notions, grâce aux différents projets qui m'ont été confié.

Je tiens également à remercier toutes l'équipe de la DTN pour leur accueil chaleureux.

Enfin, je tiens à remercier la Région Pays de la Loire pour m'avoir donné l'opportunité de réaliser cet apprentissage dans un environnement professionnel stimulant et pour m'avoir permis de renforcer ma compétence en informatique.

Je suis convaincu que cette expérience professionnelle sera d'une grande utilité pour la suite de mon parcours professionnel.

Sommaire

Remerciements.....	3
1 Présentation.....	6
2 Introduction.....	6
3 Présentation de l'entreprise et du service	6
3.1 Coordonnées de la structure d'accueil.....	6
3.2 Situation géographique	6
3.3 Repères historiques :	8
3.4 Ses activités :.....	9
3.5 Institutions – le Conseil régional des Pays de la Loire :	9
3.6 Enjeux et perspectives (2025 - 2030).....	10
3.7 Organigramme : Du service SI.....	10
3.8 Présentation du service.....	11
4 Missions réalisées en organisation :.....	11
4.1 Missions 1 : La surveillance et l'exploitation des infrastructures du système d'information de la Région	12
4.2 Missions 2 : L'installation et la gestion des serveurs applicatifs physiques et virtuels	12
4.3 Missions 3 : L'intégration et la maintenance des équipements de réseau.....	13
4.4 Missions 4 : La résolution de tickets d'incidents.....	14
5 Projet Personnalisé Encadré n°1 : Migration des LUN ISCSI vers VHDX.....	15
5.1 Contexte du Projet :.....	15
5.2 Organisation et contraintes :.....	17
5.3 Procédure réalisée pour le serveur SRV-NET-SUP-04.	19
5.3.1 Contrôle et mise à l'arrêt des services	19
5.3.2 Sauvegarde du serveur avec Veeam / Exportation du disque :.....	21
5.3.3 Désactiver le volume.....	26
5.3.4 Mise en production.....	27
5.4 Conclusion du projet :	31
6 Projet Personnalisé Encadré n°2 : Installation d'un Serveur SFTP sous Oracle Linux 9.5	32
6.1 Contexte du Projet :.....	32
6.2 Organisation et contraintes :.....	32
6.3 Création de la VM sur l'hyperviseur :	34
6.4 Installation du système d'exploitation	36
6.5 DNS.....	41
6.6 Paramétrage de la VM :.....	41
6.6.1 Configuration SNMP :	41
6.6.2 Désinstallation de Firewalld :	41

6.6.3	Installation de IPTABLES :	42
6.6.4	Configuration de IPTABLES :.....	42
6.6.5	Mise à jour :	43
6.6.6	Déploiement de l'antivirus avec Ansible :	43
6.6.7	Déploiement de la page d'accueil :	44
6.7	Configuration de la sauvegarde Veeam :.....	45
6.8	Configuration SFTP :.....	46
6.9	Supprimer l'accès en SSH au compte root :	47
6.10	Configuration du Firewall :.....	48
6.11	Configuration DNS extérieur :.....	49
6.12	Paramétrage de la supervision dans Centreon.....	50
6.13	Conclusion :	51
7	Portfolio / Site entreprise	51
8	Conclusion générale.....	52
9	ANNEXES	53
9.1	<i>Annexe 1 : Procédure d'Installation d'une VM Windows</i>	53
9.2	<i>Annexe 2 : Photo baie</i>	65

1 Présentation

Je m'appelle Corentin CHAUVEL, j'ai 20 ans et je vis dans la région Nantaise.

Mon parcours d'étude a commencé par un BAC PRO SN (systèmes numériques) Option Réseaux informatiques et systèmes communicants (RISC) étant un passionné d'informatique depuis mon adolescence. Je me voyais travailler dans cette voie, j'ai obtenu ce BAC et ai poursuivi vers un BTS SIO option solutions d'infrastructure, systèmes et réseaux (SISR) en alternance car avec les différents stages que j'ai pu effectuer au long de ces trois années à préparer le BAC, j'ai apprécié la partie entreprise.

2 Introduction

Cette alternance a été réalisé dans le cadre de mes études en BTS SIO, au sein du service informatique de la Région Pays de la Loire.

Cette période a été l'occasion pour moi de découvrir les différents aspects de l'informatique dans un environnement professionnel et plus particulièrement en administration système et réseaux. J'ai pu mettre en pratique les connaissances acquises lors des cours et découvrir de nouvelles technologies.

Ce rapport a pour objectif de présenter les différentes missions qui m'ont été confiées au cours de cette alternance, ainsi que les compétences et les connaissances que j'ai développées. Il permettra de mettre en évidence les solutions mises en place.

3 Présentation de l'entreprise et du service

3.1 Coordonnées de la structure d'accueil

Hôtel de Région des Pays de la Loire
Adresse : 1 Rue de la Loire, 44000 Nantes
Téléphone : 02 28 20 50 00
Site : <https://www.paysdeloire.fr/>

3.2 Situation géographique

Située à l'ouest de la France, entre Bretagne, Centre Val de Loire et Nouvelle Aquitaine, la région Pays de la Loire regroupe cinq départements : Loire Atlantique, Maine et Loire, Mayenne, Sarthe et Vendée. Chef-lieu : Nantes où est situé l'Hôtel de la Région des Pays de La Loire. La région s'appuie sur un double ancrage littoral et ligérien : une façade atlantique stratégique (ports, énergies marines, tourisme) et le plus long fleuve de France, la Loire (agriculture, paysages, patrimoine).

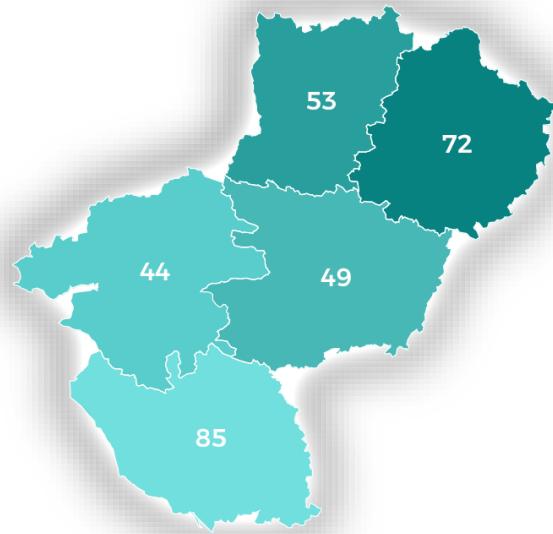


Figure 1 : Région Pays de la Loire

L'hôtel de la Région se situe sur l'île Beaulieu dans le centre de Nantes.

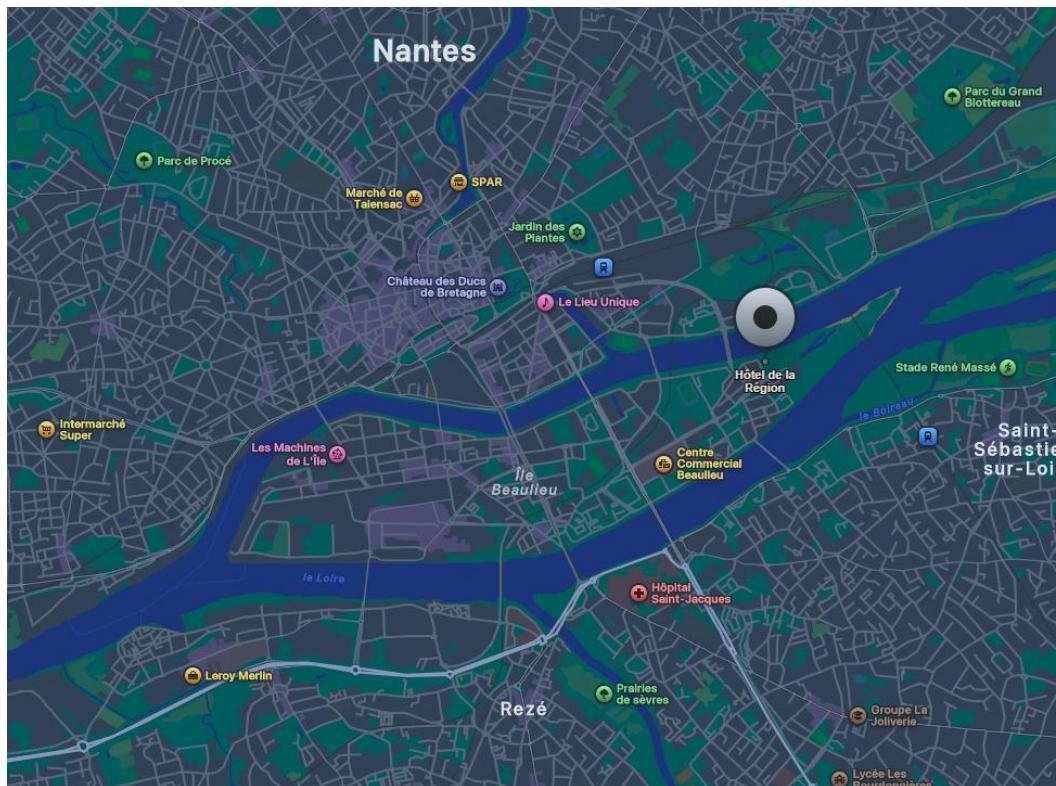


Figure 2: L'hôtel de la Région est desservi par plusieurs lignes de bus et est facilement accessible en voiture



Figure 3 : Maison de la région (Il y en a au moins une dans chaque département.)

3.3 Repères historiques :

Avant 1950 : territoire structuré par d'anciennes provinces (Anjou, Maine, Poitou occidental, Bretagne pour la Loire-Atlantique), des villes comptoirs sur l'Atlantique (Nantes, Saint-Nazaire) et des bassins agricoles réputés (Anjou/Val de Loire, bocages du Maine et de la Vendée).

1955-1972 : l'État dessine des « régions de programme » pour l'aménagement du territoire ; 1972 crée l'Établissement public régional (EPR) en Pays de la Loire.

1982 : lois de décentralisation (lois « Defferre ») ; la région devient collectivité territoriale de plein exercice.

1986 : premières élections régionales au suffrage universel direct ; la politique régionale s'autonomise (formation, lycées, transports régionaux, développement économique...)

Depuis 2000 : montée en puissance des compétences (transports régionaux, apprentissage, stratégie économique), contractualisation avec l'État/UE, planification durable, affirmation de filières d'excellence industrielles, agroalimentaires, nautiques et numériques.

3.4 Ses activités :

Économie : aides aux entreprises, soutien à l'innovation, attractivité du territoire.

Formation & lycées : construction et entretien des lycées, financement de l'apprentissage, orientation professionnelle.

Transports : organisation et financement des trains régionaux (TER), cars interurbains, mobilité durable.

Aménagement du territoire : gestion du Schéma régional d'aménagement (SRADDET), équilibre entre zones rurales, urbaines et littorales.

Environnement & énergie : développement des énergies renouvelables, adaptation au changement climatique, biodiversité.

Culture, sport et patrimoine : soutien aux festivals, musées, bibliothèques, clubs sportifs de haut niveau.

Gestion des fonds européens : redistribution des aides européennes.

3.5 Institutions – le Conseil régional des Pays de la Loire :

Création et statut : EPR en 1972 ; collectivité territoriale depuis 1982 ; élections régionales au suffrage universel direct depuis 1986.

Siège : Hôtel de Région, Nantes.

Composition : 93 conseillers régionaux (scrutin de liste à deux tours, prime majoritaire).

Fonctionnement : assemblée délibérante (séances plénières, votes budgétaires), commissions sectorielles, exécutif régional (Présidente et vice-présidences), services et agences (ex. Solutions & Co pour le développement éco).

Présidences depuis l'origine :

- Olivier Guichard : 1974-1998.
- François Fillon : 1998-2002.
- JeanLuc Harousseau : 2002-2004.
- Jacques Auxiette : 2004-2015.
- Bruno Retailleau : 2015-2017.
- Christelle Morançais : 2017 en cours (réélue en 2021).

Chantiers actuels (exemples)

- Transition écologique (rénovation thermique, décarbonation industries/ports, mobilités propres, biodiversité).
- Compétences et emploi : apprentissage, orientation, métiers en tension.

- Mobilités : modernisation TER, liaisons côtières/estuariennes, intermodalité métros/bus/tram.
- Économie : soutien aux filières (naval, aéronautique, agroalimentaire, numérique), export, innovation, foncier économique.

3.6 Enjeux et perspectives (2025- 2030)

Transition écologique juste : adaptation littorale, ressource en eau, risques Loire/affluents, sobriété foncière et énergétique.

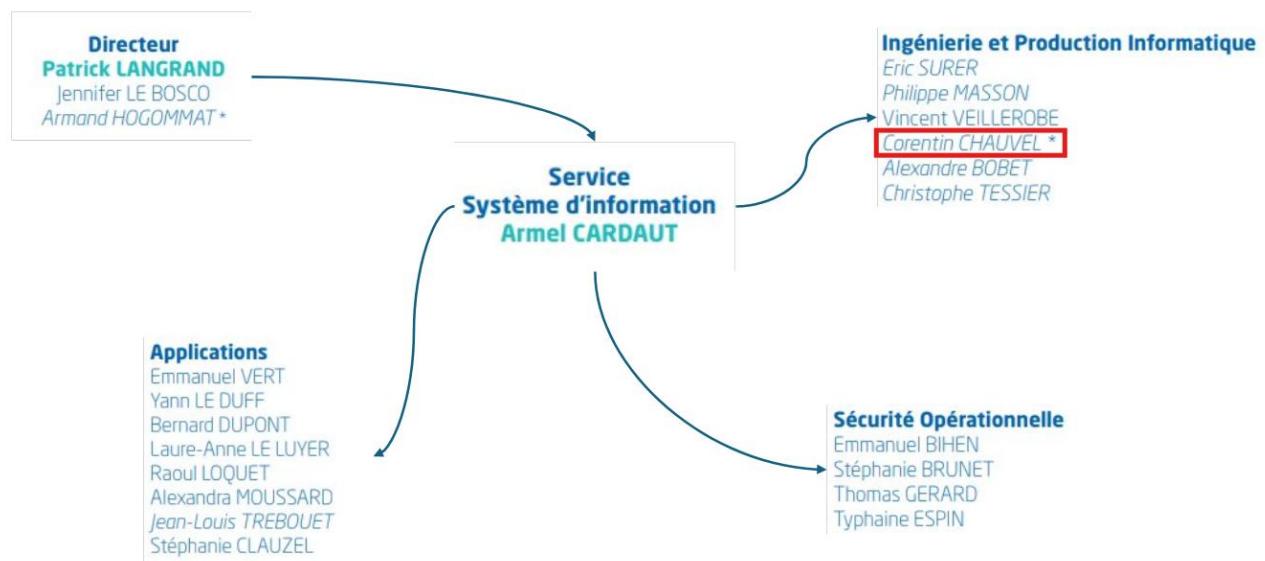
Compétences & attractivité : répondre aux besoins en BTP industrie santé, requalification, mix apprentissage/formation continue, inclusion, logement des actifs/étudiants.

Mobilités & cohésions : régénération ferroviaire/TER, intermodalité métropolitaine, desserte des territoires ruraux et littoraux, décarbonation logistique/ports.

Innovation & productivité : accélérer l'industrialisation verte (naval/EMR, agro transformation, électronique de puissance), diffusion numérique/IA dans les PME, recherche transfert, export.

Équilibres territoriaux : métropolisation vs Ruralité, littoral vs arrière-pays, politique de villes moyennes et centralités.

3.7 Organigramme : Du service SI



3.8 Présentation du service

Le service système d'Information (SSI) est composé de 19 personnes avec différents pôles, Ingénierie et Production Informatique, Sécurité Opérationnelle et Applications. Dans le pôle où je me situe (Ingénierie et Production Informatique) mon tuteur Vincent VEILLEROBE s'occupe de l'administration des systèmes et équipements réseaux, l'administration du stockage et l'administration des systèmes de virtualisation. Dans le pôle tout le monde a sa petite spécialité : gestion des mises en production, sauvegardes et restaurations, supervision du SI, gestion des bases de données relatives aux applications, gestion des traitements informatiques. Dans le pôle Sécurité Opérationnelle il s'occupe de la gestion des infrastructures de sécurité du système d'information, l'administration réseau, gestion d'office 365 et Azure AD, l'administration systèmes Microsoft, expertise PowerShell, AD et bien sur la téléphonie. Et le pôle application qui gère les applications de finances et les différents applications internes. Je travaille au quotidien avec tous ces personnes. Le pôle Ingénierie et Sécurité travaillent de façon étroite (les réunions sont conjointes).

4 Missions réalisées en organisation :



Ci-dessous, j'explique 4 missions que j'effectue au quotidien. Ces différentes tâches demandent un suivi régulier.

4.1 Missions 1 : La surveillance et l'exploitation des infrastructures du système d'information de la Région

La surveillance de notre infrastructure informatique est assurée à l'aide de l'outil Centreon. Cet outil nous permet de superviser l'ensemble des équipements du réseau, tels que les switchs, routeurs, onduleurs, ainsi que les serveurs physiques, les machines virtuelles (VM), certaines applications et des URLs critiques.

L'un des principaux avantages de Centreon est la centralisation des informations sur une seule interface, ce qui nous permet d'avoir une vue d'ensemble claire et en temps réel de l'état de notre système d'information.

Nous avons également mis en place un système d'alertes personnalisées en fonction de certains seuils critiques. Par exemple, une alerte est générée si un disque dur approche de sa capacité maximale, si la RAM est fortement sollicitée sur une période prolongée, ou encore en cas de perte de connectivité (ping), de désynchronisation NTP, etc. Ces alertes nous permettent d'être proactifs et d'intervenir rapidement avant que des incidents n'impactent les utilisateurs.

Host & SVC Monitoring

Host Monitoring (Visu 100 lignes max)

Host Name	Status	Duration	Tries	Status information
	DOWN	3w 4d ago	5/3 (1)	CRITICAL: 404 Not Found
	DOWN	2w 8d ago	1/3 (1)	CRITICAL: 404 Not Found
	DOWN	4d 9h ago	1/3 (1)	OK - demo disksh (R:13.17B/s lost:0%)

Service Monitoring (Visu 100 lignes max)

S	Host Name	Service	Status	Duration	Hard State Duration	Last Check	Tries	Status Information
1		HTTP-Response-Time	Critical	2w 3d ago	2w 3d ago	2m 7s ago	3/3 (H)	CRITICAL: 500 Can't connect to tsmvelco.paysdel
2		Disks	Critical	1m 1w ago	1m 1w ago	4m 11s ago	3/3 (H)	CRITICAL: 1\:\ 21B/1B used
3		Swap	Critical	4d 14h ago	4d 14h ago	11m 47s ago	3/3 (H)	CRITICAL: Used: 98.64 %
4		Memory	Critical	2h 25m ago	2h 25m ago	5m 51s ago	3/3 (H)	CRITICAL: physical free: 279016B used: 29.201GB si
5		Ntp	Critical	11s ago	11s ago	11s ago	3/3 (H)	CRITICAL: Time offset: -3 second(s) Local Time: -2
6		Load	Critical	2h 25m ago	2h 25m ago	1m 49s ago	3/3 (H)	CRITICAL: Load average: 8.23, 7.72, 7.39
7		Storage-J	Critical	1w 2d ago	1w 2d ago	5m 7s ago	3/3 (H)	CRITICAL: Storage: 7 Usage Total: 19.94 GB Used:
8		Disk-Global	Critical	1w 2d ago	1w 2d ago	7m 36s ago	3/3 (H)	CRITICAL: Storage: 7 Usage Total: 19.94 GB Used:
9		Memory	Critical	1h 17m ago	1h 17m ago	2m 15s ago	3/3 (H)	CRITICAL: physical free: 760.586MB used: 7.256GB si
10		Memory	Critical	23h 45m ago	23h 45m ago	15m ago	3/3 (H)	CRITICAL: physical free: 281.063MB used: 3.744GB si
11		Interface-G20/4	Critical	2d 12h ago	2d 12h ago	1m 41s ago	3/3 (H)	CRITICAL: Interface G20/4 Status: down (admin)
12		Disks	Critical	1w 1d ago	1w 1d ago	50s ago	3/3 (H)	CRITICAL: C:\ 93.527GB/97.296GB used
13		Memory	Critical	12h 12m ago	12h 12m ago	12m 21s ago	3/3 (H)	CRITICAL: physical free: 658.988MB used: 7.356GB si

Figure 4 : Centreon outil de supervision

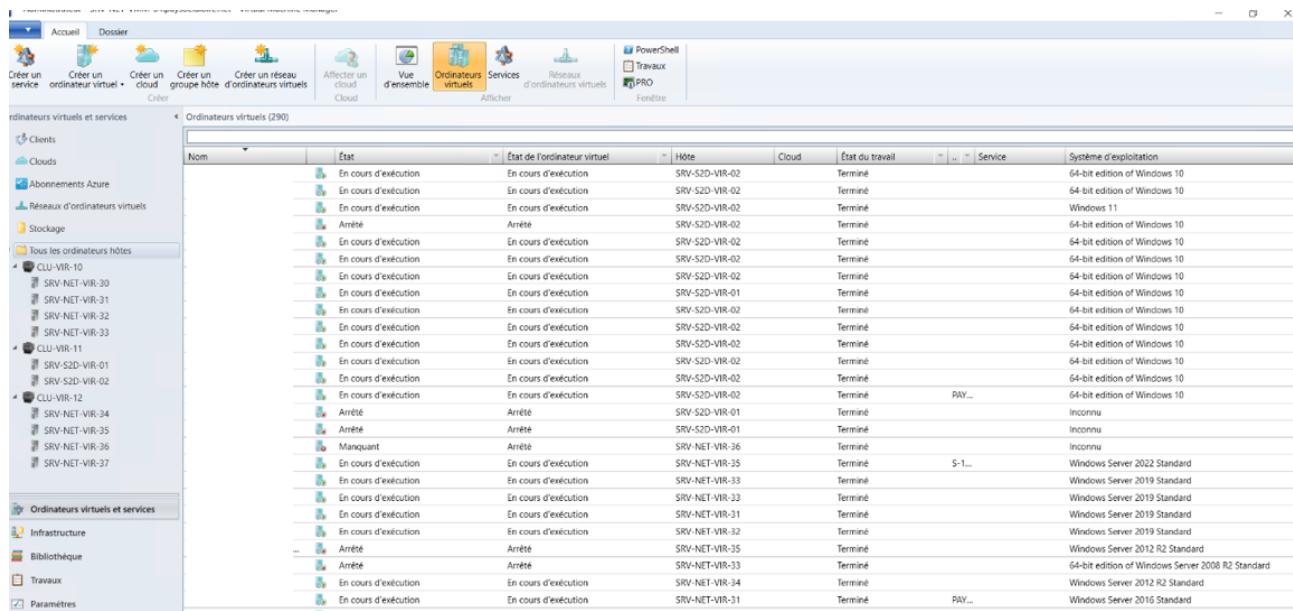
4.2 Missions 2 : L'installation et la gestion des serveurs applicatifs physiques et virtuels

Je suis en charge de l'installation et de la gestion des serveurs applicatifs, qu'ils soient physiques ou virtuels sous Windows ou Linux. Cela comprend notamment le déploiement, la configuration et le maintien des serveurs nécessaires au bon fonctionnement des applications métiers.

Selon les besoins, certaines applications ou services peuvent devoir être déployés afin d'assurer le bon fonctionnement de l'application qui sera exécutée sur la machine virtuelle.

Je m'occupe également de la gestion des machines virtuelles (VM), depuis leur création jusqu'à leur supervision, en passant par l'attribution des ressources (CPU, RAM, stockage) sur nos hyperviseurs.

Voir l'annexe 1 pour la documentation que j'ai faite pour l'installation d'une VM Windows qui avait besoin d'être accessible par le WALLIX Bastion.



The screenshot shows the SCVMM interface with the following details:

- Top Bar:** Accueil, Dossier, Createur d'ordinateur virtuel, Createur d'un cloud, Createur d'un groupe hôte, Createur d'un réseau d'ordinateurs virtuels, Affecteur d'un cloud, Vue d'ensemble, Ordinateurs virtuels (highlighted in orange), Services, Réseaux d'ordinateurs virtuels, PowerShell, Travaux, PRO, Fenêtre.
- Left Sidebar:** Ordinateurs virtuels et services, Clients, Clouds, Abonnements Azure, Réseaux d'ordinateurs virtuels, Stockage, Tous les ordinateurs hôtes, CLU-VIR-10, CLU-VIR-11, CLU-VIR-12, SRV-NET-VIR-30, SRV-NET-VIR-31, SRV-NET-VIR-32, SRV-NET-VIR-33, SRV-NET-VIR-34, SRV-NET-VIR-35, SRV-NET-VIR-36, SRV-NET-VIR-37.
- Central Table:** Titled "Ordinateurs virtuels (290)", it lists 290 virtual machines. The columns are: Nom, État, État de l'ordinateur virtuel, Hôte, Cloud, État du travail, Service, Système d'exploitation.

Figure 5: SCVMM (System Center Virtual Machine Manager) est utilisé pour gérer les machines virtuelles au sein des différents clusters.

4.3 Missions 3 : L'intégration et la maintenance des équipements de réseau

Dans le cadre de l'intégration de nouveaux serveurs, j'ai été amené à réaliser le brassage réseau nécessaire à leur mise en service, ainsi que la configuration des switchs associés, aussi bien pour le réseau LAN (Local Area Network) que pour la DMZ (zone démilitarisée).

J'ai notamment participé à la configuration des ports, à l'attribution des VLANs, et à la vérification de la connectivité réseau via des tests. Ce travail s'est fait en collaboration avec l'équipe sécurité opérationnelle, en suivant les normes internes de câblage et de sécurité.

À Laval, j'ai eu l'opportunité de contribuer à la mise en place du réseau dans l'un des nouveaux bâtiments. Cela a impliqué le brassage physique d'une partie du bâtiment, c'est-à-dire le raccordement des différentes prises RJ45 vers les baies de brassage et leur conformité au schéma réseau prévu.

Viennent ensuite les petits problèmes du quotidien, comme l'installation de nouveaux pilotes pour les cartes Wi-Fi afin de résoudre des problèmes de déconnexion lors des tests. Il y a aussi des interventions, comme le brassage de prises pour améliorer la gestion des connexions, ou encore le tri dans les baies réseau pour réorganiser les connexions sur les switchs et libérer de la place.

Ces interventions m'ont permis d'approfondir mes compétences pratiques en infrastructure réseau, notamment sur les aspects de câblage structuré (voir annexe 2), configuration de switchs, segmentation réseau (via VLAN) et la gestion de la connectivité des équipements actifs.

4.4 Missions 4 : La résolution de tickets d'incidents

Comme logiciel de ticketing, à la Région nous utilisons ISILOG, un logiciel de gestion de maintenance assistée par ordinateur (GMAO) qui nous permet d'optimiser l'ensemble de nos opérations de maintenance.

Le logiciel offre un suivi rigoureux de chaque intervention réalisée, en enregistrant les actions effectuées, les pièces consommées ainsi que les coûts associés. Cette traçabilité complète nous permet de disposer d'un historique précis, facilitant l'analyse des performances et la mise en place d'améliorations ciblées.

Par ailleurs, ISILOG nous permet de gérer de manière centralisée notre parc matériel ainsi que les stocks, assurant ainsi une disponibilité optimale des ressources nécessaires à la maintenance.

A la Région, il y a un service support qui est chargé de gérer l'ensemble des incidents de premier niveau. Lorsqu'ils rencontrent des problèmes qu'ils ne peuvent pas résoudre, ou lorsqu'ils ne disposent pas des droits nécessaires pour intervenir, ils transmettent les tickets au SSI. Nous prenons alors le relais pour traiter ces demandes plus complexes ou nécessitant des accès spécifiques.

Parmi les tickets que je traite au quotidien, on retrouve par exemple le déblocage de compte utilisateur sur le VPN ainsi que d'e-mails retenus par notre pare-feu de messagerie, la gestion des accès aux répertoires partagés, ou encore les demandes d'accès à certains serveurs. Je suis également amené à intervenir sur des problèmes de performance, comme des lenteurs constatées sur un serveur : dans ce cas, je réalise différents tests et vérifications afin d'identifier l'origine du dysfonctionnement et proposer des solutions adaptées.

Cela peut également concerner une demande de brassage/réseau. Par exemple, un réfrigérateur connecté était initialement en Wi-Fi et rencontrait des problèmes de déconnexion. Je l'ai donc raccordé en filaire afin d'assurer une connexion plus stable.

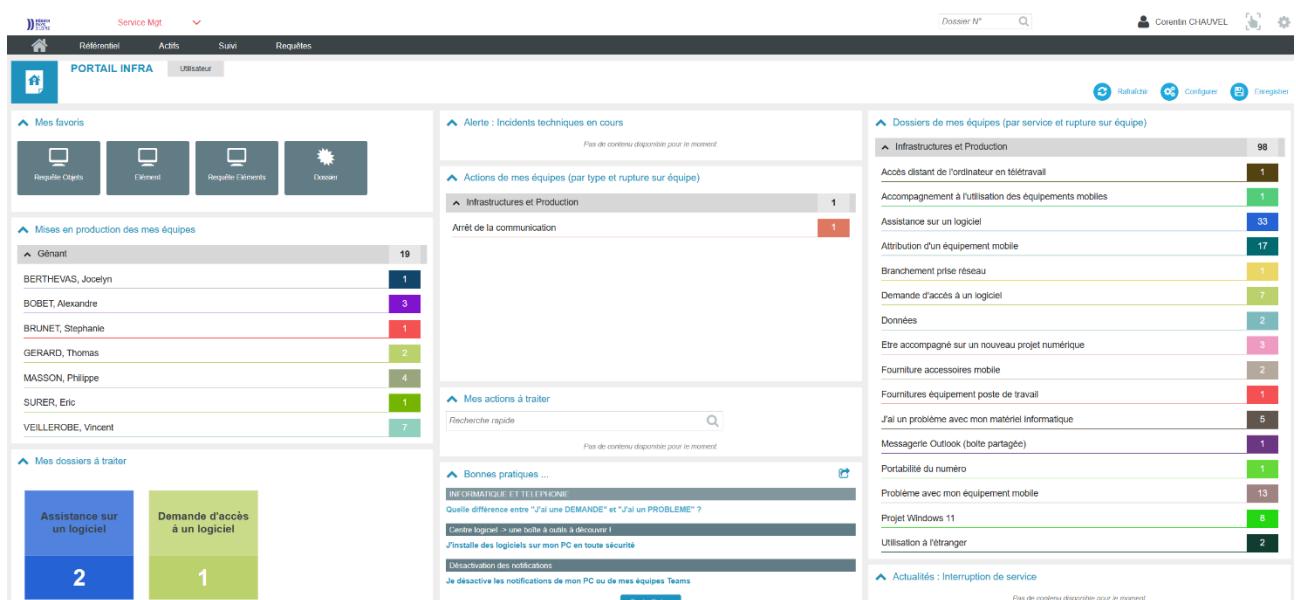


Figure 6 : Logiciel de ticketing ISILOG

5 Projet Personnalisé Encadré n°1 : Migration des LUN iSCSI vers VHDX

5.1 Contexte du Projet :

Dans le cadre de la modernisation de l'infrastructure virtuelle et de la préparation à l'arrivée des nouveaux serveurs Hyper-V 2025, il a été décidé d'unifier l'architecture de stockage des machines virtuelles (VM) existantes.

Actuellement, certains serveurs utilisent un disque système (C:) au format VHDX, stocké sur un volume réseau (Microsoft Cluster Storage Volume) hébergé sur une baie NetApp en MetroCluster (une configuration qui protège les données grâce à deux clusters en miroir situés sur des sites distincts).

En revanche, leurs disques de données (E:, F:, G:, etc.) ne sont pas au format VHDX : ils sont directement connectés sous forme de LUN iSCSI, chaque disque étant associé à un volume dédié portant le nom du serveur sur la baie NetApp.

Afin d'assurer une meilleure homogénéité, de simplifier la gestion et de garantir une compatibilité totale avec les futurs hôtes Hyper-V, l'ensemble de ces disques doit être converti au format VHDX et hébergé sur des volumes réseau accessibles depuis tous les hôtes Hyper-V.

Cette approche permettra également de supprimer les multiples LUN iSCSI créées individuellement pour chaque disque de données, rendant la gestion des volumes sur la baie NetApp bien plus simple et centralisée.

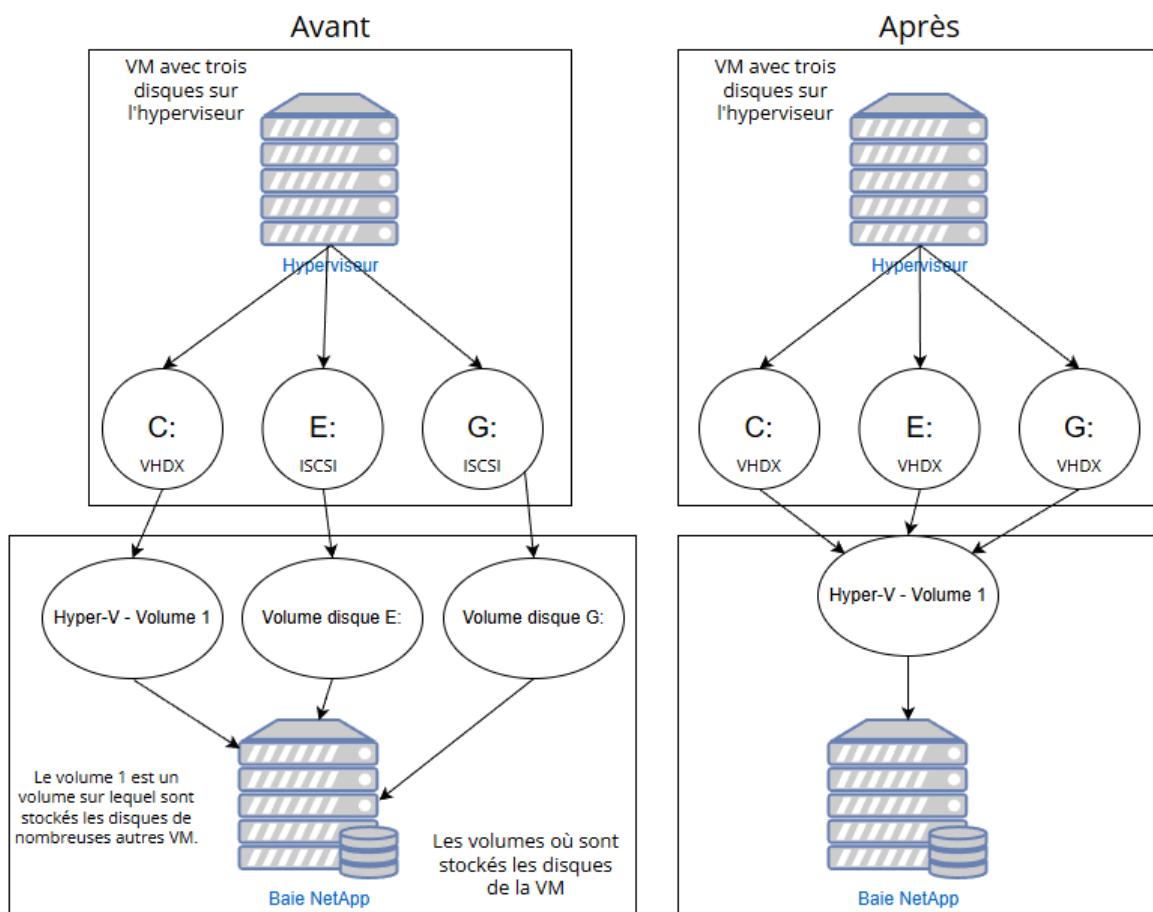


Figure 7 : Voici un schéma permettant d'illustrer clairement la différence entre la situation "avant" et "après".

Le format VHDX est un fichier qui représente un disque dur virtuel. Il contient le système d'exploitation, les partitions et les données, et il est utilisé principalement avec l'hyperviseur Hyper-V.

Une LUN iSCSI (Logical Unit Number via iSCSI) est un disque virtuel présenté à un serveur à travers le protocole iSCSI. Elle est hébergée sur une baie de stockage NetApp et apparaît pour le serveur comme un disque physique local, alors qu'il est en réalité distant.

À l'inverse, l'iSCSI est un protocole qui permet d'accéder à un disque situé sur une baie de stockage distante via le réseau, comme s'il était directement connecté physiquement au serveur.

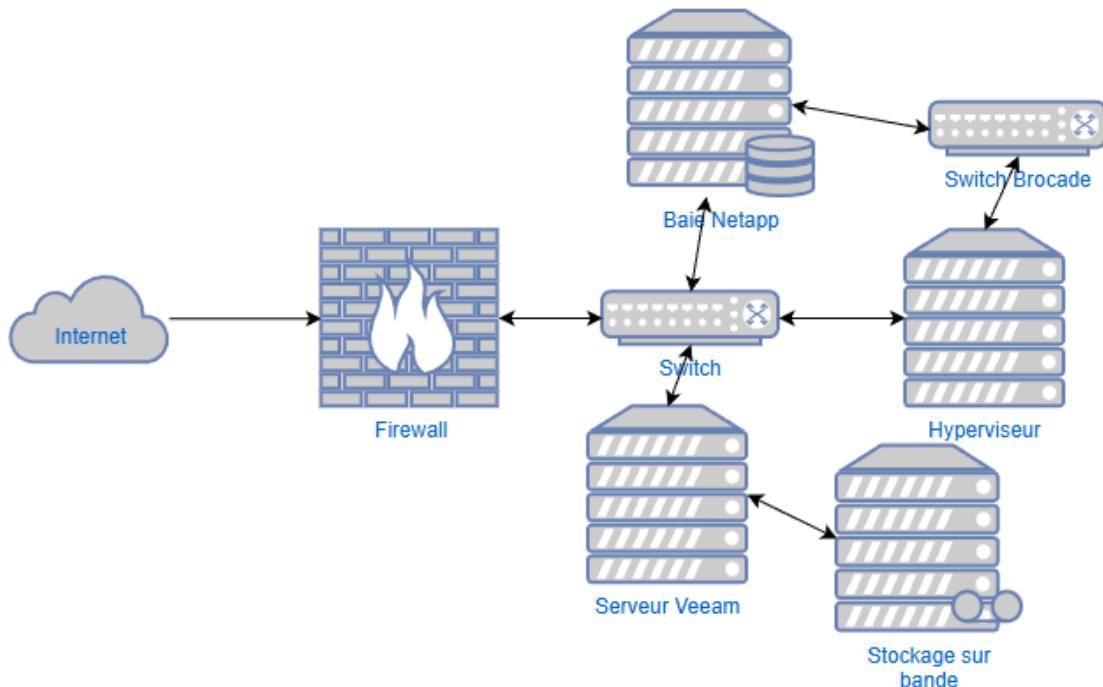


Figure 8 : Schéma simplifié du réseau et du matériel utilisés pour le projet après la migration.

Il est important de préciser que le switch Brocade utilisé est un switch Fibre Channel dédié. Les hyperviseurs sont connectés à la baie NetApp via des liens Fibre Channel 16 Gbit/s, et non via un réseau IP classique. Ce choix assure des performances élevées, une latence minimale et une meilleure fiabilité. Dans cette architecture, la connexion entre le serveur Veeam et la solution de stockage sur bande est également réalisée en Fibre Channel.

5.2 Organisation et contraintes :

Cette opération nécessite l'arrêt temporaire des services applicatifs hébergés sur les serveurs concernés. Chaque coupure a donc dû être planifiée en concertation avec les responsables applicatifs, puis communiquée via un avis d'intervention envoyé aux utilisateurs par mail.

Bonjour,

Une opération est planifiée sur le SI.

Merci de considérer cette opération et son implication dans vos missions et de nous faire part de toute incompatibilité.

Objet de l'opération : Migration disque Iscsi vers Vhdx du serveur SRV-MDM-BDD-01

Application(s) impactée(s) : application mdm

L'assistance doit envoyer un mail aux utilisateurs : Non, Romain Vallet se charge de prévenir les utilisateurs

Texte du mail :

Directions ou clients impactés :

Date et heure d'opération : 23/04/2025 à 14H

Durée de l'opération : 1 H

Interruption de service : oui

Type d'intervention (patch, mise à jour, modification de paramétrage...) :

Objectif(s) de la mise à jour (correction de bug, apports fonctionnels, correctif technique...) :

Serveurs impactés : SRV-MDM-BDD-01

Responsable(s) de l'opération : Corentin CHAUVEL

Cordialement,

Figure 9 : Exemple de mail envoyez pour prévenir les utilisateurs.

Une fois les validations obtenues, les opérations ont été planifiées et réalisées sur une période allant du 16 avril 2025 au 28 avril 2025.

De plus, certains serveurs possèdent des disques de plus de 2 To, ce qui peut rendre l'opération longue, environ six heures.

C'est une opération délicate et il a fallu rester très attentifs tout le long de ce projet surtout pendant les migrations.

Dans un premier temps, j'ai constitué un fichier Excel pour centraliser les différentes données : quels serveurs sont concernés, qui utilise chaque serveur, quelles applications y fonctionnent. Ensuite, j'ai identifié quels disques étaient à migrer.

Une fois toutes les informations recueillies, j'ai pu débuter la planification des différents créneaux d'intervention. Pour cela, j'ai structuré l'avancement sous forme de projet dans un fichier Excel, présenté au format diagramme de Gantt.

MIGRATION ISCSI->VHDX

DIAGRAMME DE GANTT

REGION Pays de la Loire
Chef de projet : Corentin CHAUVEL

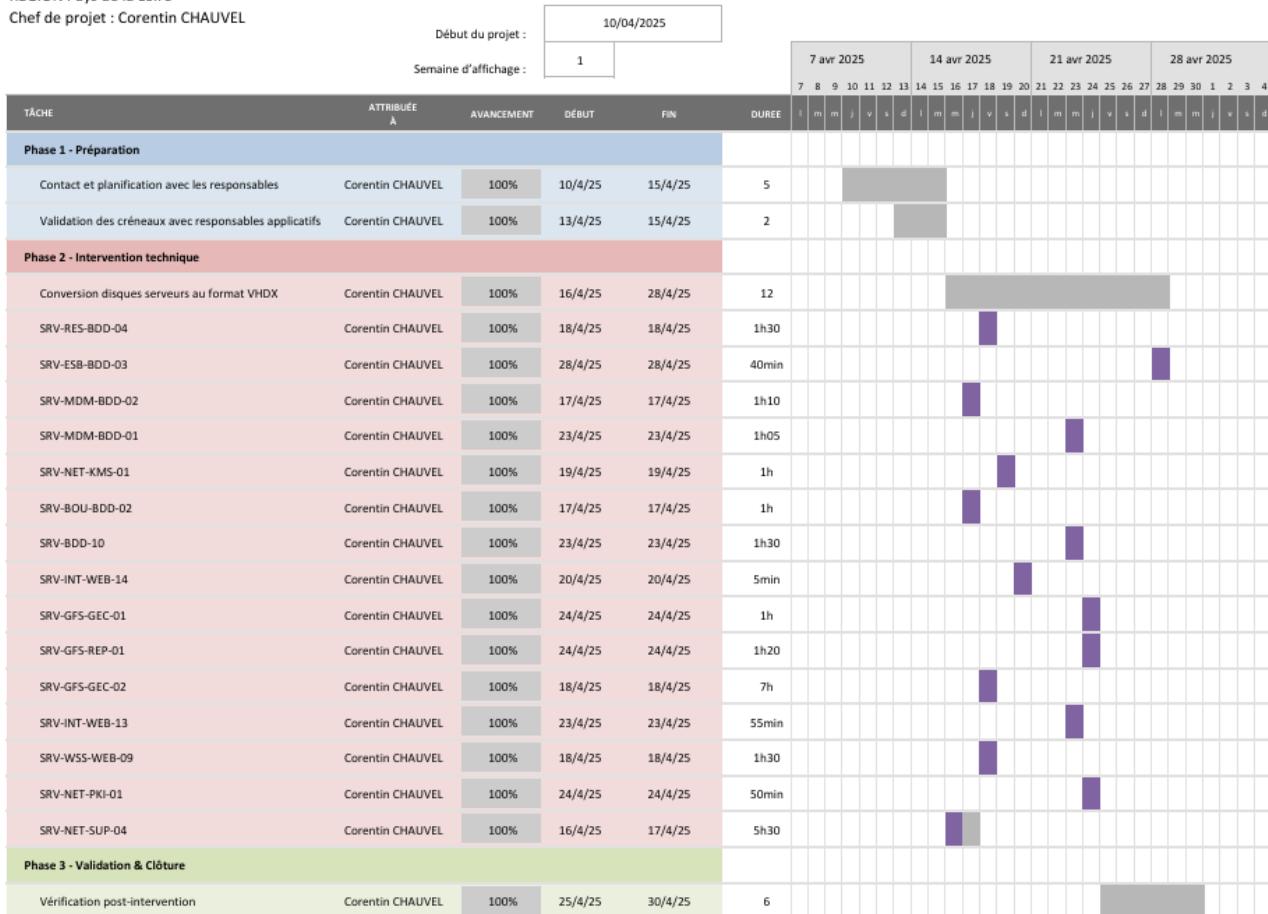


Figure 10 : Gantt

Pour réaliser cette opération, plusieurs étapes sont nécessaires. Elle commence par la sauvegarde du serveur via Veeam, puis l'extraction du ou des disques au format VHDX depuis le serveur de sauvegarde. Une fois ces disques récupérés, ils sont ajoutés dans la console SCVMM. Enfin, il est indispensable de redémarrer les différents services en fonction des rôles et des applications présents sur le serveur afin de rétablir son fonctionnement normal.

Voici le déroulement de la procédure de migration. Elle sera identique pour l'ensemble des serveurs, à l'exception de quelques ajustements selon les services en cours d'exécution et le nombre de disques connectés en iSCSI.

5.3 Procédure réalisée pour le serveur SRV-NET-SUP-04.

5.3.1 Contrôle et mise à l'arrêt des services

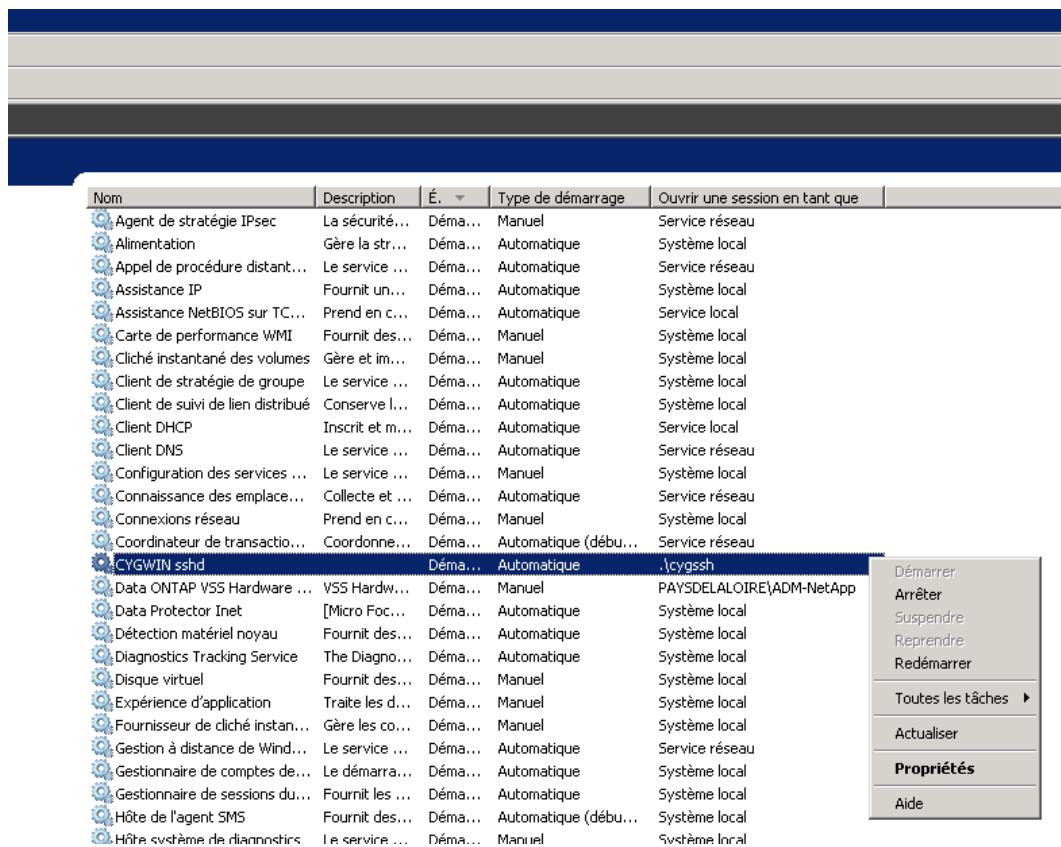
D'abord, connexion sur le serveur de sauvegarde Veeam :

Si dans la colonne Backup Agent, il est noté « Reboot required », alors il faut redémarrer le serveur en question, c'est que l'agent Veeam n'a pas totalement installé. Puis faire un « Rescan » dans Veeam pour vérifier que l'installation c'est bien effectuée.

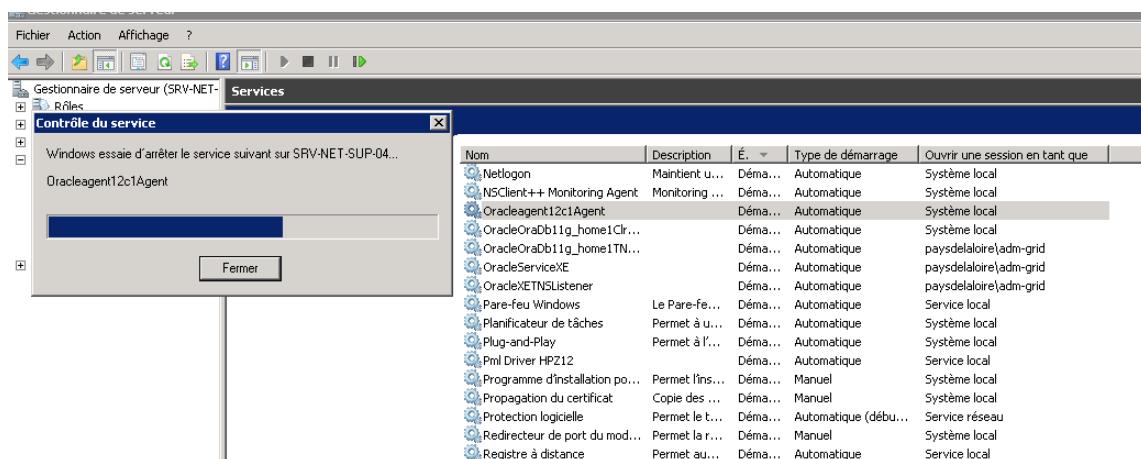
The screenshot shows the Veeam Backup & Replication interface. The 'Inventory' tab is selected. In the left sidebar, under 'Malware Detection (29)', the 'Servers Windows iSCSI' node is selected and highlighted with a red box. In the main list, the 'SRV-NET-SUP-04.paysdelaloire.net' host is listed with 'Reboot required' in the 'Backup Agent' column. A red box highlights the 'Rescan' option in the context menu for this host. The 'Actions' menu for this host is open, showing 'Reboot required', 'Rescan' (highlighted with a red box), 'Reboot', 'Quick backup', 'Add to backup job', 'Agent', 'Plug-in', 'Uninstall everything', 'Remove from configuration', and 'Details...'.

The screenshot shows the 'Machine rescan' dialog box. It displays a table of hosts and their status. The 'SRV-NET-SUP-04.paysdelaloire.net' host is listed with a status of 'Success'. A red box highlights the 'Installed' status for this host in the 'Status' column. The 'Message' column shows a green checkmark and the text: 'Job started at 16/04/2025 14:43:01', 'Performing rescan', '1 host processed', and 'Job finished at 16/04/2025 14:43:14'. The 'Duration' column shows '0:00:10'.

Connexion au serveur que l'on vient de redémarrer, pour arrêter les services de l'application qui sont en cours d'exécution sur le serveur. Ouvrir le gestionnaire de serveur et se diriger dans Services.



Par exemple sur cette machine il faut arrêter « CYGWIN sshd » et les différents services Oracle. Pour d'autres serveurs, ce sont les services SQL ; cela dépend de l'utilisation du serveur et de l'application.



5.3.2 Sauvegarde du serveur avec Veeam / Exportation du disque :

Sur le serveur, effectuez un clic droit puis sélectionnez Quick Backup afin de lancer une sauvegarde instantanée. Avant cela, j'ai arrêté les services en cours d'exécution sur le serveur afin de garantir une sauvegarde la plus propre et fiable possible.

Dans Veeam Backup & Réplication, Quick Backup est une fonctionnalité qui permet de lancer rapidement une sauvegarde incrémentielle d'une machine virtuelle (VM) ou d'un objet sans devoir refaire une session complète de sauvegarde.

Cela s'appuie sur le dernier point de sauvegarde existant pour n'enregistrer que les changements récents.

The screenshot shows the Veeam Backup & Replication interface. On the left, the 'Inventory' pane is open, displaying a tree view of the environment. The 'Virtual Infrastructure' section is expanded, showing 'Microsoft Hyper-V' and 'SCVMM Servers' with several hosts listed. The 'Physical Infrastructure' section is also expanded, showing various servers and storage units. The 'Out of Date' section shows 3 items. The 'Backup Infrastructure' section is collapsed. At the bottom, there are navigation buttons for 'Home', 'Inventory' (which is selected and highlighted in blue), and 'Backup Infrastructure'.

The main pane shows a list of hosts with columns for 'Name', 'IP Address', 'Last Seen', and 'Backup Agent'. A host named 'SRV-NET-SUP-04.paysdelaloire.net' is selected and highlighted in blue. A context menu is open for this host, with the 'Quick backup' option highlighted with a red box. Other options in the menu include 'Rescan', 'Add to backup job', 'Agent', 'Plug-in', 'Uninstall everything', 'Remove from configuration', and 'Details...'. The 'IP Address' column for the selected host shows '10.144.10.18' and 'Online'.

Figure 11 : Quick backup

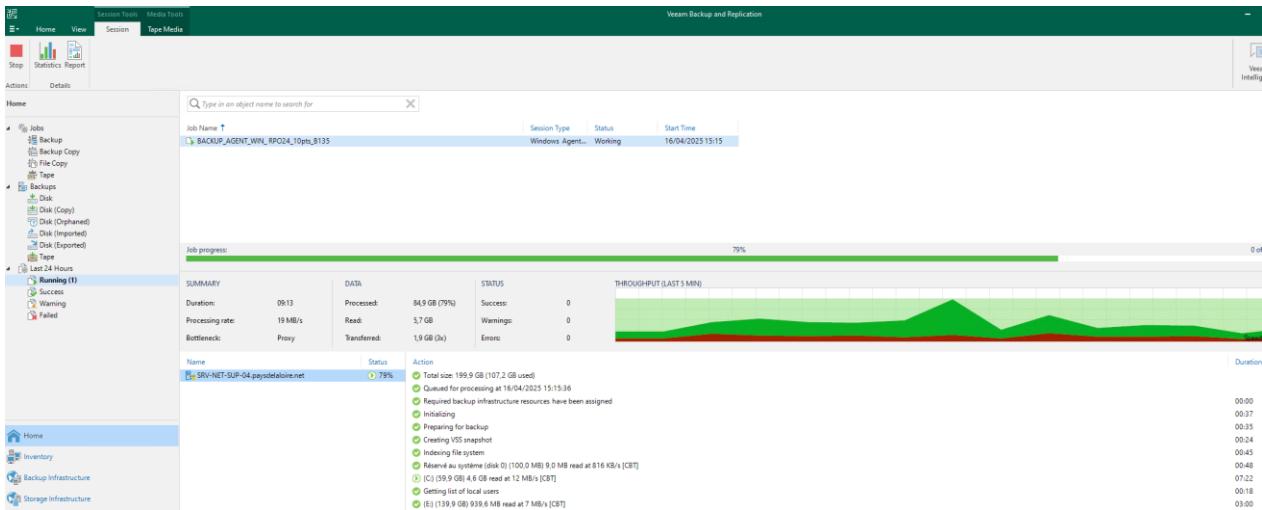
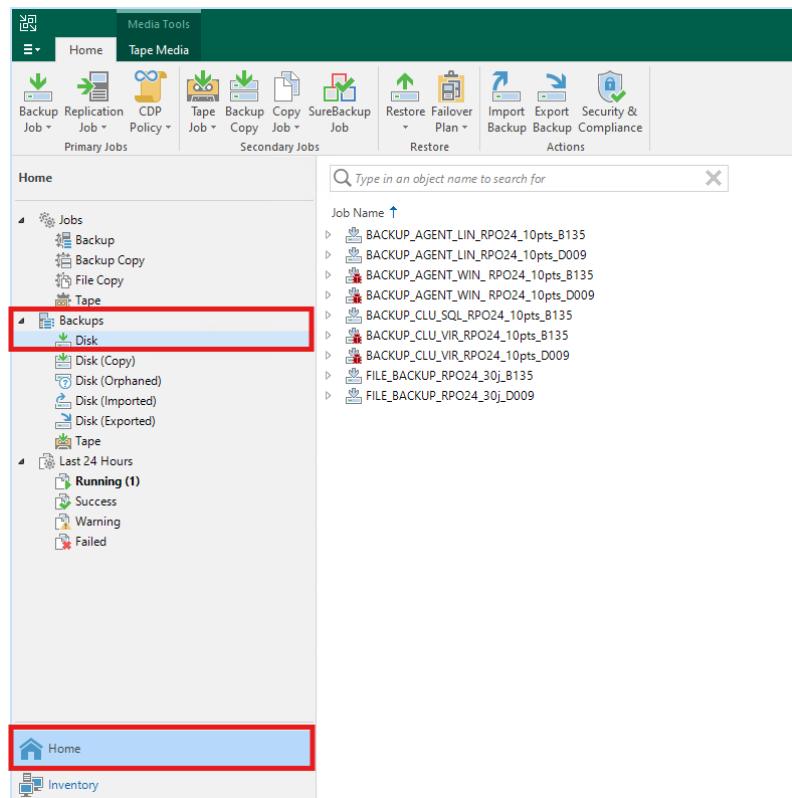


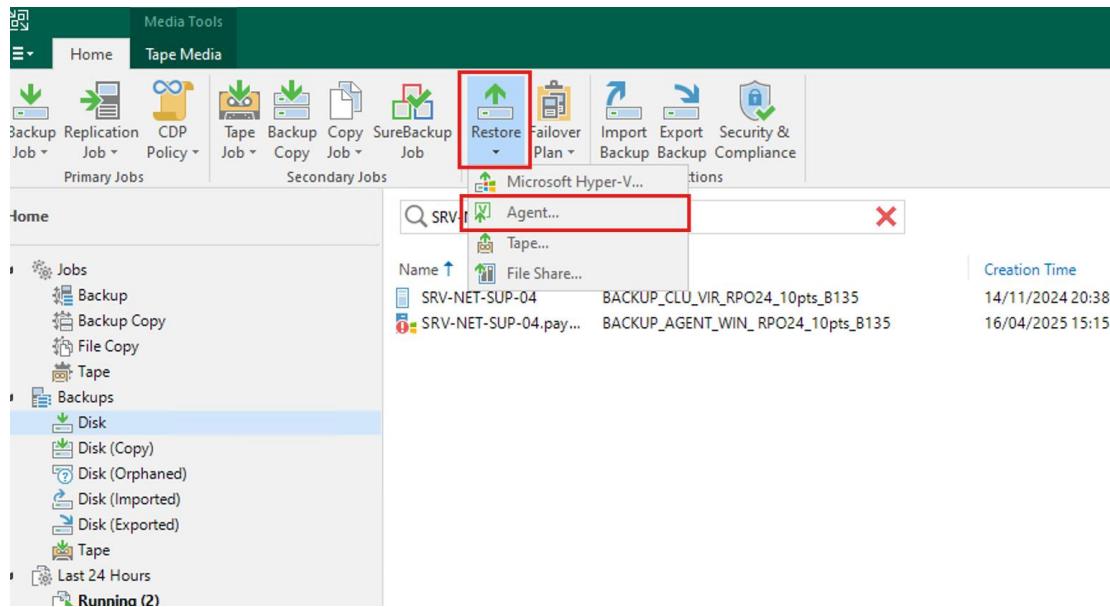
Figure 12 : Vu de l'avancement de la sauvegarde.

Une fois la sauvegarde finie, il faut extraire une copie du disque qui est en lscsi.

Ci-dessous j'explique les différentes actions à mener :



Ensuite effectuer : Restore > Agent



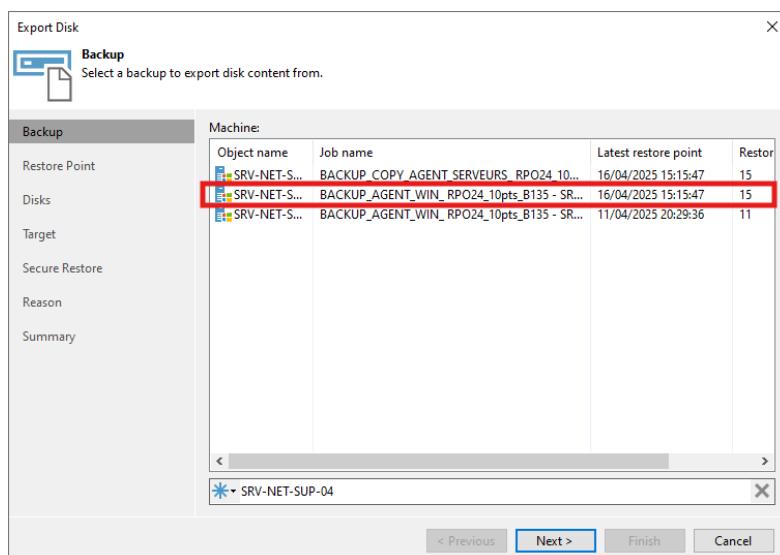
Restore from Veeam Agent backup
Select the type of restore you want to perform.

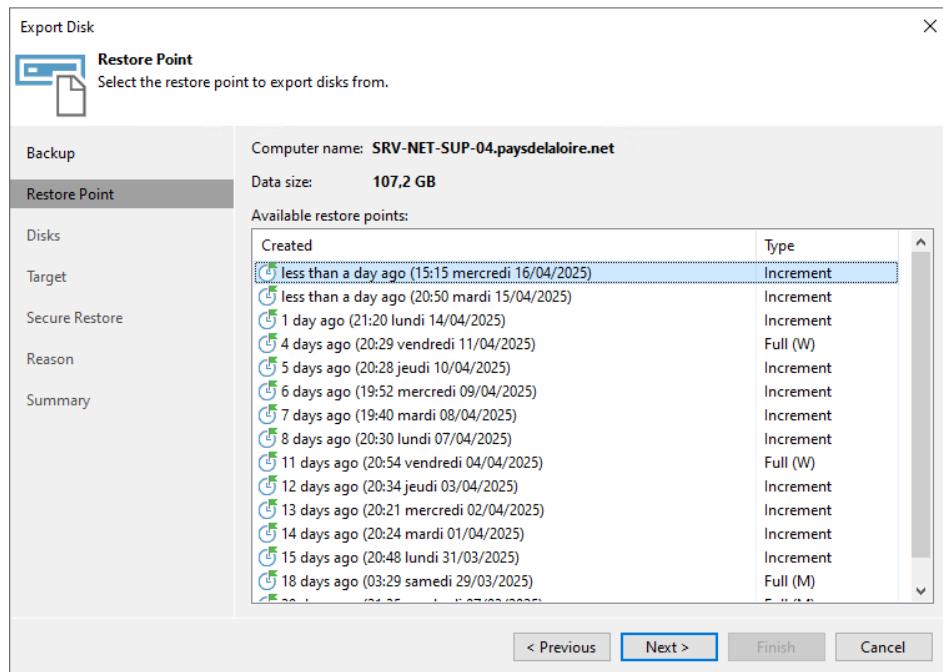
- Entire machine restore**
Restores backup as a virtual or cloud machine.
- Disk restore**
Restores the content of individual disks and volumes. **Disk restore** is highlighted with a red box.
- Guest files restore**
Restores individual guest files from an image-level backup.
- Application items restore**
Restores individual application items from an image-level backup.
- Database restore**
Restores databases to a point in time back to the original or to a different server.

Disk Restore
Select the type of restore type you want to perform.

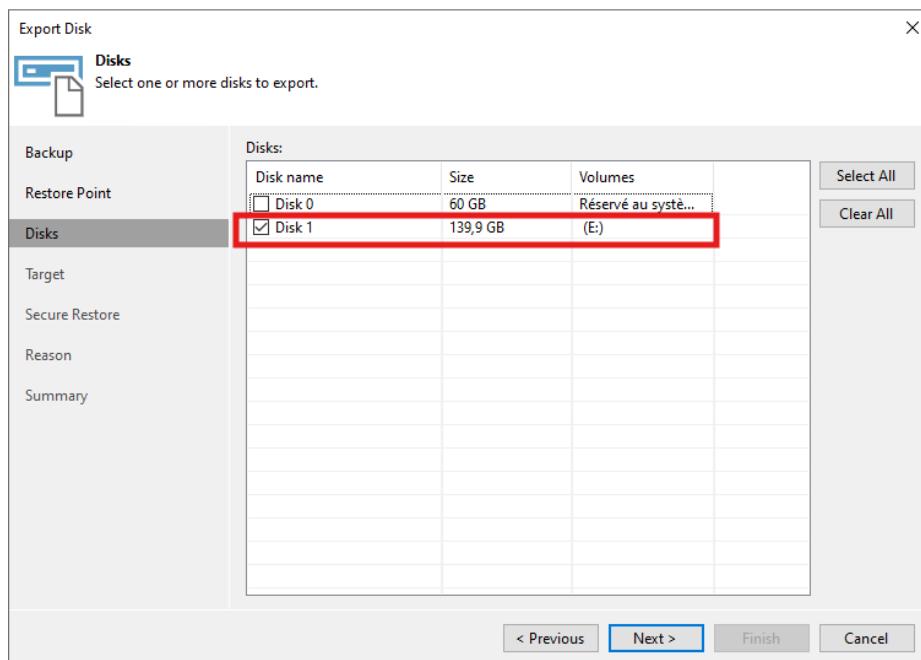
- Volume restore**
Restores individual volumes to the selected server or workstation.
- Export disk**
Exports disk content as a virtual disk file of the selected format. **Export disk** is highlighted with a red box.
- Publish disk**
Instantly publishes backed up disk content to any machine as a new volume. Any changes made to the disk content will be discarded when the disk is unpublished.

Choisir le dernier backup : celui qui vient d'être fait et pas la copie.

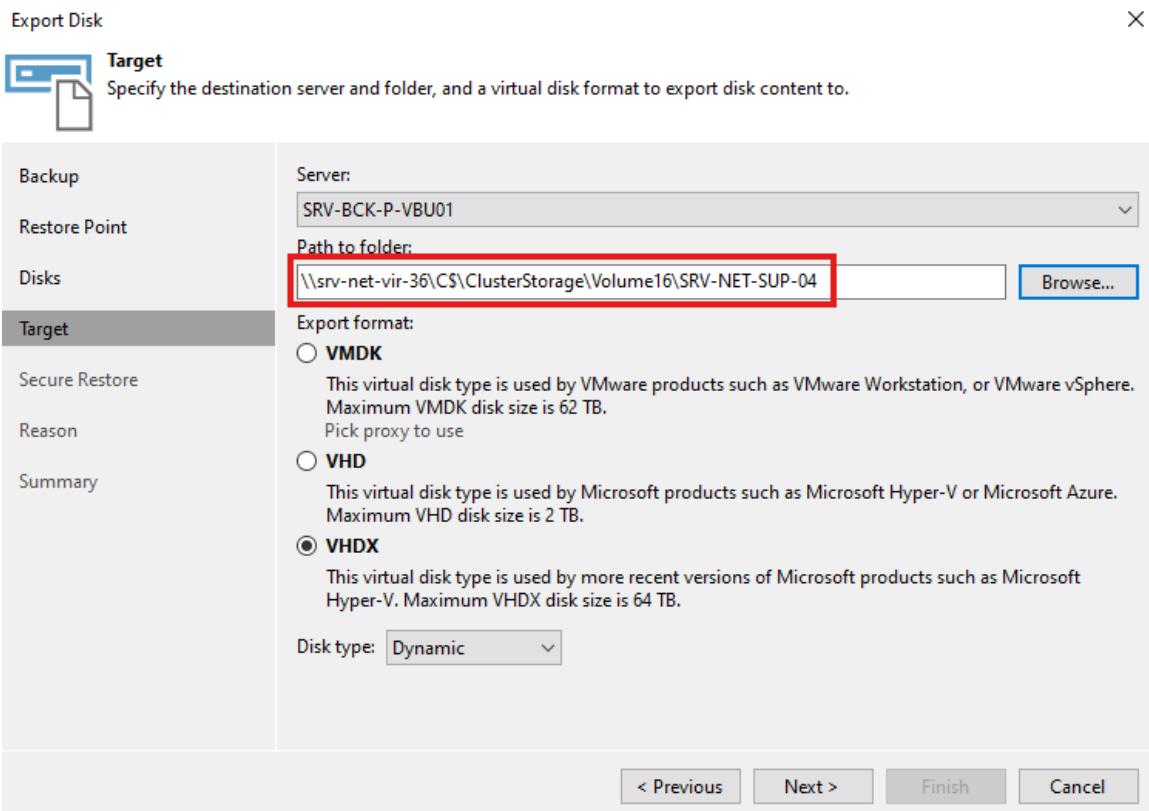




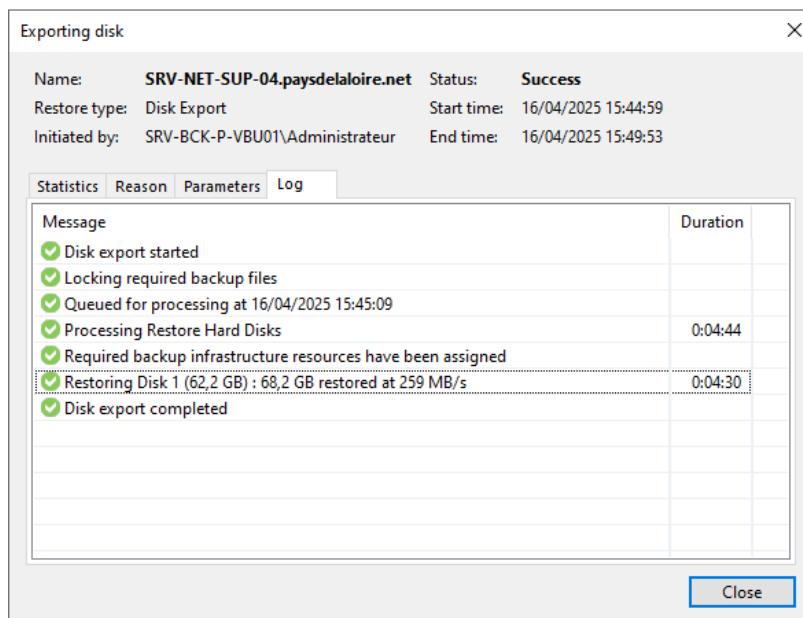
Choisir le ou les disque(s) qui est en lscsi concerné, cela dépend des serveurs et de combien de disque y sont.



Mettre directement le chemin vers l'emplacement du serveur où est stocké le disque C du serveur, en ayant auparavant vérifier sur quel volume se situe le stockage de la VM, ensuite choisir le format VHDX.



Ci-dessous : capture indiquant que l'export s'est bien déroulé (toutes les coches sont vertes) :



5.3.3 Désactiver le volume

Une baie NetApp regroupe des disques en agrégats RAID pour créer des volumes logiques qui servent de base au stockage. Ces volumes peuvent ensuite être partagés via différents protocoles comme NFS, SMB, iSCSI ou Fibre Channel.

Ensuite connexion à la baie NetApp pour désactiver le volume.

Soit sur la baie en B135 ou en D009, en fonction de celle sur laquelle le volume se situe.

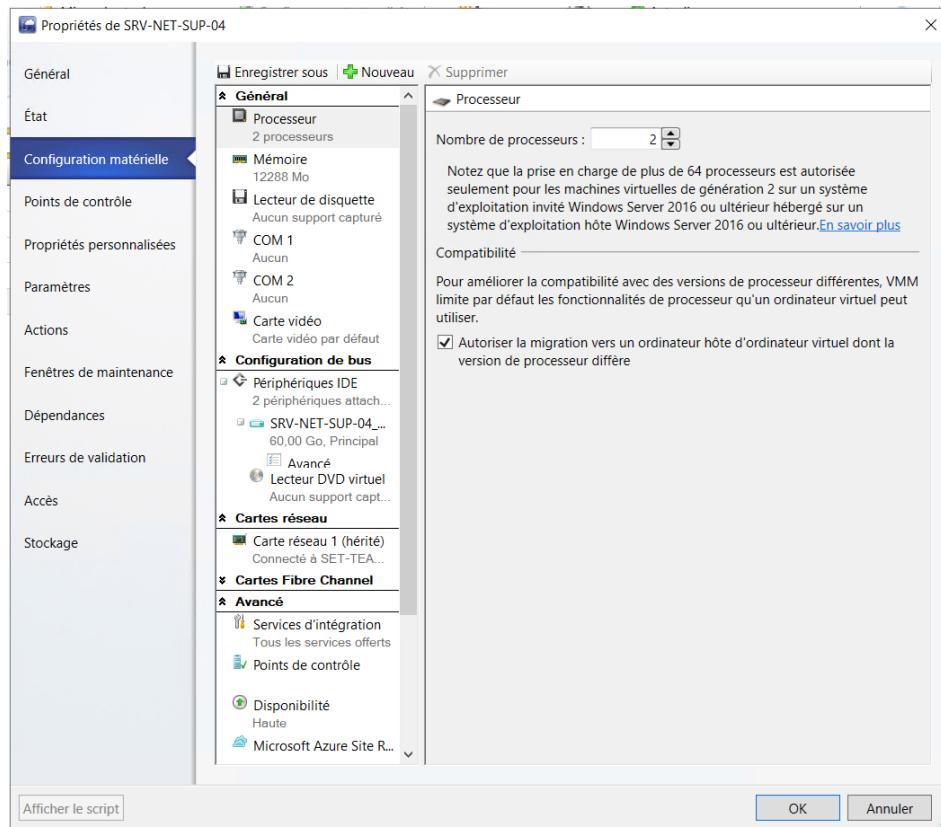
ONTAP System Manager		Search actions, objects, and pages			
Dashboard		Volumes			
INSIGHTS		+ Add		More	
Storage	▼	Name	Storage VM	Status	Capacity
Overview	▼	srv_esb_bdd_01	srv-sto-ata-05	Online	8,98 GiB used <div style="width: 80%; background-color: #0070C0; height: 10px; margin-left: 10px;"></div> 6,02 GiB available 15 GiB 0
Volumes	▼	srv_esb_bdd_02	srv-sto-ata-05	Online	8,77 GiB used <div style="width: 80%; background-color: #0070C0; height: 10px; margin-left: 10px;"></div> 6,23 GiB available 15 GiB 0
LUNs	▼	srv_esb_bdd_03	srv-sto-ata-05	Online	53,4 GiB used <div style="width: 80%; background-color: #0070C0; height: 10px; margin-left: 10px;"></div> 26,6 GiB available 80 GiB 0
Consistency Groups	▼	srv_gfs_rep_01	srv-sto-ata-05	Online	37,4 GiB used <div style="width: 80%; background-color: #0070C0; height: 10px; margin-left: 10px;"></div> 62,6 GiB available 100 GiB 5
NVMe Namespaces	▼	srv_mdmi_bdd_01	srv-sto-ata-05	Online	50,8 GiB used <div style="width: 80%; background-color: #0070C0; height: 10px; margin-left: 10px;"></div> 19,2 GiB available 70 GiB 0
Shares	▼	srv_mdmi_bdd_02	srv-sto-ata-05	Online	94,2 GiB used <div style="width: 80%; background-color: #0070C0; height: 10px; margin-left: 10px;"></div> 25,8 GiB available 120 GiB 2
Buckets	▼	srv_mgx_vdi_03	srv-sto-ata-05	Online	332 GiB used <div style="width: 80%; background-color: #0070C0; height: 10px; margin-left: 10px;"></div> 87,5 GiB available 420 GiB 0
Qtrees	▼	srv_my_bdd_01	srv-sto-ata-05	Online	18,6 GiB used <div style="width: 80%; background-color: #0070C0; height: 10px; margin-left: 10px;"></div> 21,4 GiB available 40 GiB 0
Quotas	▼	srv_net_pk1_01	srv-sto-ata-05	Online	32,4 GiB used <div style="width: 80%; background-color: #0070C0; height: 10px; margin-left: 10px;"></div> 37,6 GiB available 70 GiB 0
Storage VMs	▼	srv_net_sup_04	srv-sto-ata-05	Offline	<div style="width: 80%; background-color: #C0C0C0; height: 10px; margin-left: 10px;"></div> 180 GiB 0
Tiers	▼	srv_pab_bdd_01	srv-sto-ata-05	Online	79,1 GiB used <div style="width: 80%; background-color: #0070C0; height: 10px; margin-left: 10px;"></div> 30,9 GiB available 110 GiB 0
Network	▼				
Events & Jobs	▼				
Protection	▼				
Hosts	▼				
Cluster	▼				

5.3.4 Mise en production

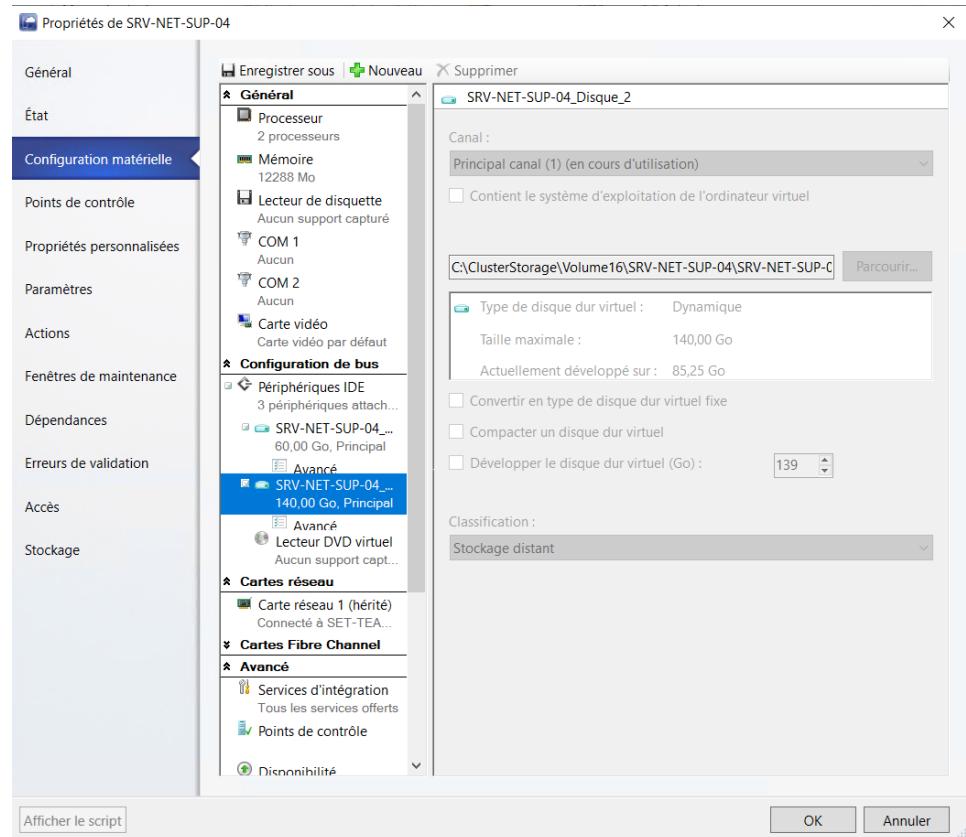
Ensuite, arrêtez le serveur, puis accédez à la console SCVMM et ouvrez les propriétés du serveur.

SCVMM signifie System Center Virtual Machine Manager. C'est une console de gestion développée par Microsoft, intégrée à la suite Microsoft System Center. Elle permet aux administrateurs informatiques de gérer, déployer et surveiller des environnements de virtualisation, basés sur Hyper-V.

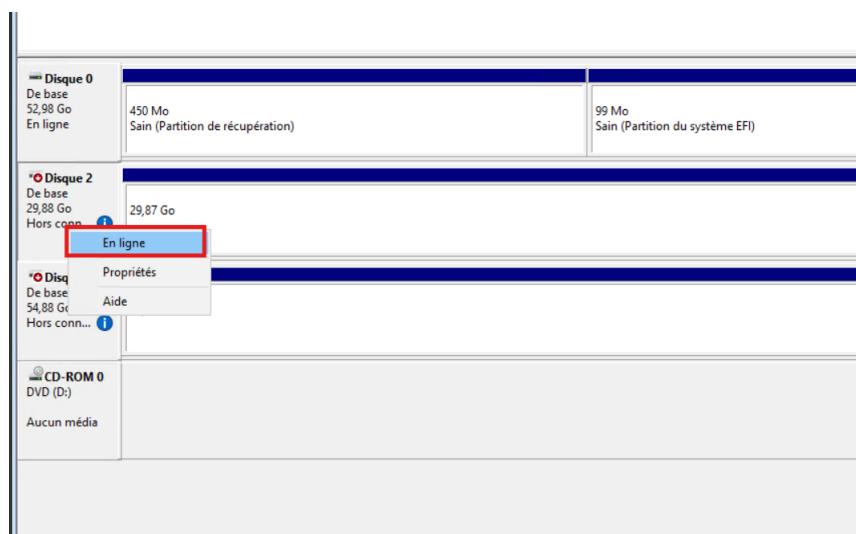
Supprimez la carte réseau n°2, qui permettait d'établir un lien direct avec la baie NetApp. Veillez à conserver la carte réseau n°1 afin que la machine maintienne son accès au réseau.

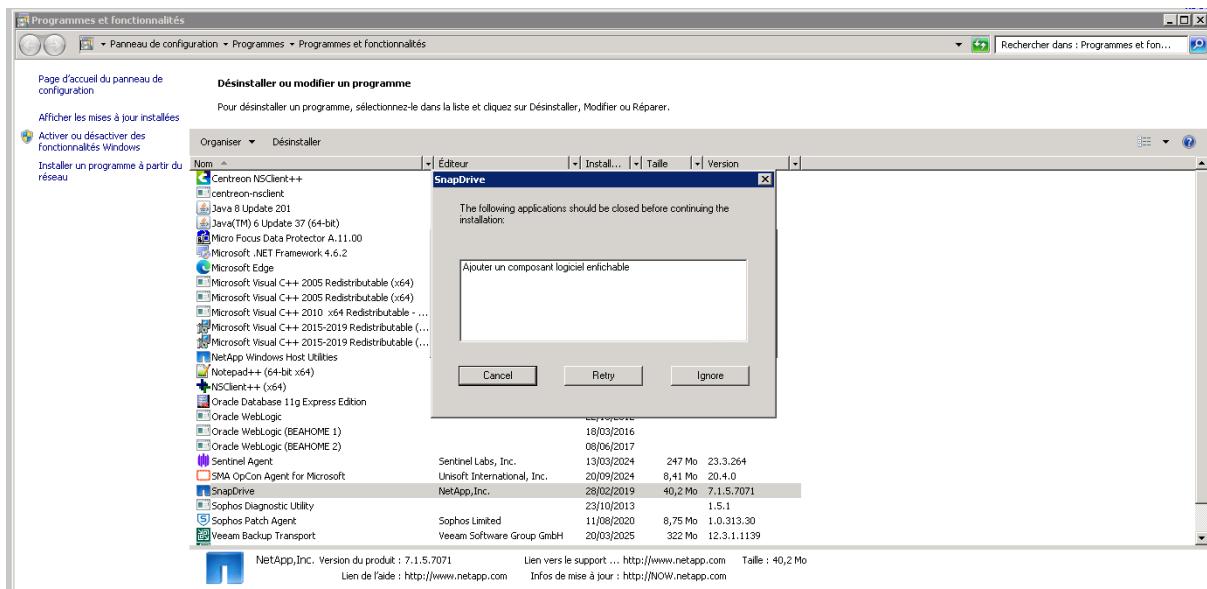


Ajoutez le disque à la machine virtuelle en sélectionnant celui récupéré à l'emplacement précédemment copié via le logiciel Veeam. Redémarrez ensuite la machine. Les services arrêtés précédemment se relancent automatiquement, mais il est important de vérifier qu'ils ont bien redémarré.



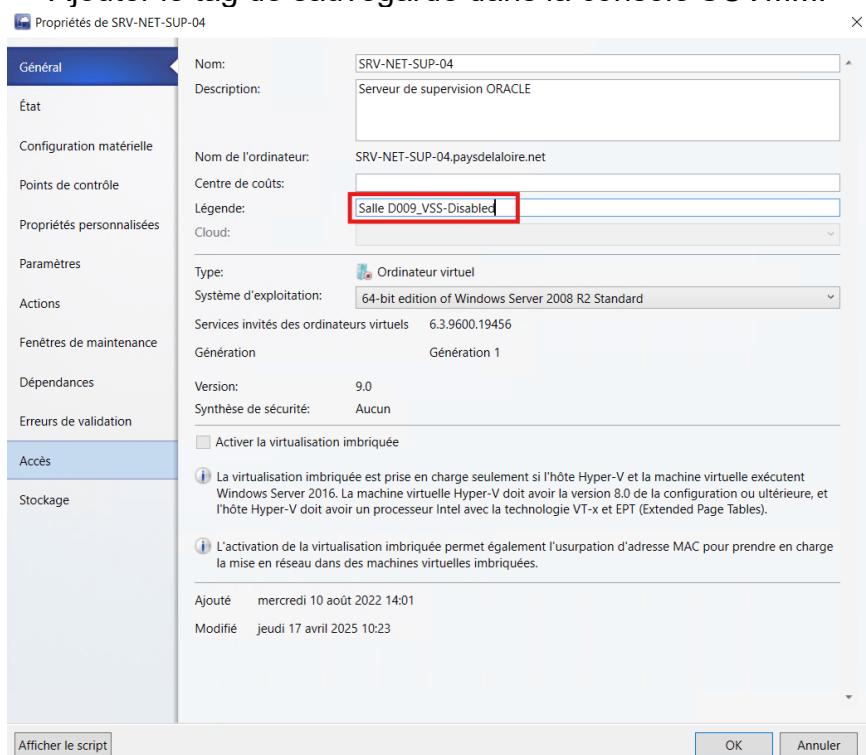
Connexion au serveur, dans le gestionnaire de disques, mettez le nouveau disque en ligne et vérifiez qu'il est bien accessible.





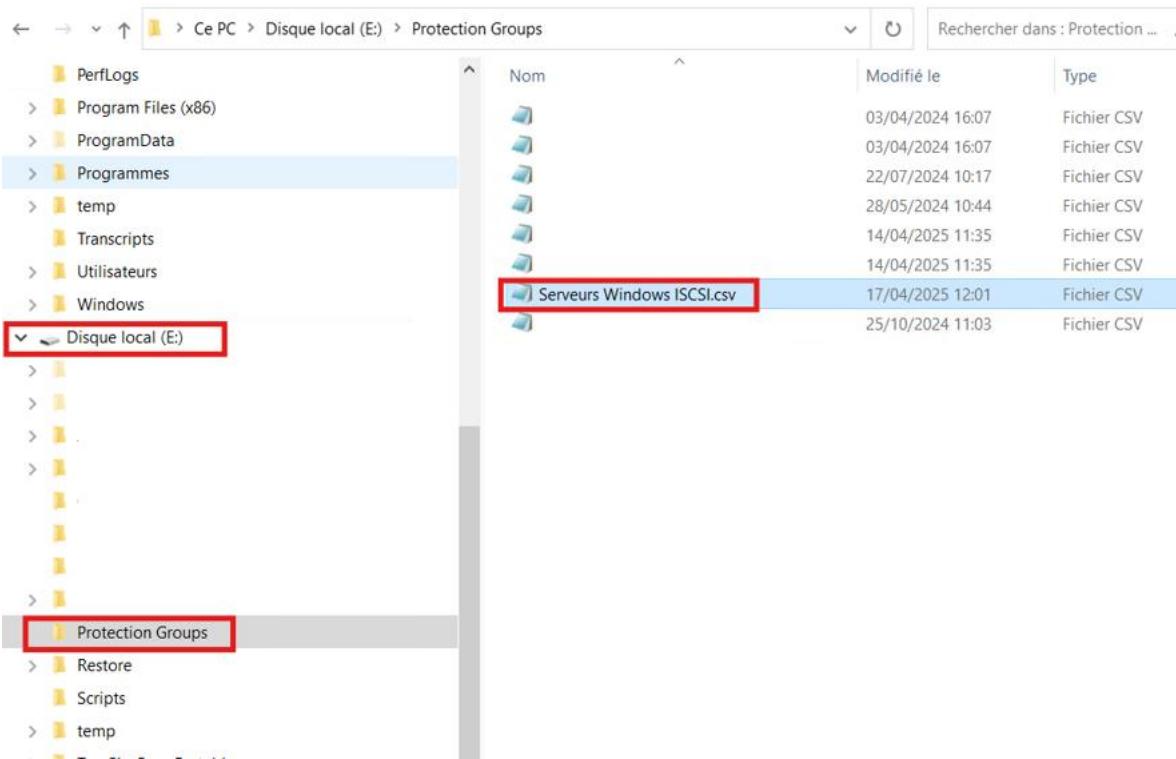
Désinstallez ensuite SnapDrive, NetApp ainsi que les agents Veeam présents sur le serveur, car la machine sera désormais sauvegardée directement par l'hyperviseur.

Ajouter le tag de sauvegarde dans la console SCVMM.



Salle D009_VSS-Disabled ou Salle B135_VSS-Disabled c'est pour la répartition de charge entre les deux bâtiments. L'outil Veeam s'appuie sur cette configuration pour effectuer la répartition des sauvegardes.

Dans Veeam sur l'explorateur de fichier suppression du serveur dans le fichier Serveurs Windows iSCSI pour qu'il ne soit plus sauvegardé de cette façon, maintenant il sera sauvegardé avec le Tag dans la Légende.



Le lendemain de la migration (pour mémoire les sauvegardes s'effectuent le soir), vérifier dans Veeam que le serveur a bien été sauvegardé avec le tag.

Name	Type	Obj
Backup Manuel	Windows Agent Backup	1
BACKUP_AGENT_LIN_RPO24_10pts_B135	Linux Agent Backup	2
BACKUP_AGENT_LIN_RPO24_10pts_D009	Linux Agent Backup	2
BACKUP_AGENT_WIN_RPO24_10pts_B135	Windows Agent Backup	2
BACKUP_AGENT_WIN_RPO24_10pts_D009	Windows Agent Backup	2
BACKUP_CLU_VIR_RPO24_10pts_B135	Hyper-V Backup	2
BACKUP_CLU_VIR_RPO24_10pts_D009	Hyper-V Backup	2
FILE_BACKUP_RPO24_30j_B135		
FILE_BACKUP_RPO24_30j_D009		

SUMMARY

Duration:	02:30:19
Processing rate:	748 MB/s
Bottleneck:	Source

Name **Status**

SRV-NET-ADC-02	Success
SRV-GFE-APL-01	Success
Modele_Windows_2019	Success
SRV-NET-SUP-09	Success

Dans l'outil des sauvegardes, on peut générer un rapport pour voir comment elles se sont déroulées. Une fois le rapport généré, utiliser « CTRL + F » pour effectuer une recherche. Entrer le nom du serveur SRV-NET-SUP-04.

Server	Result	Start	End
SRV-NET-STB-02	Success	19:03:58	19:05:07
SRV-NET-SUP-04	Success	18:07:13	18:08:14
SRV-NET-SUP-06	Success	19:05:44	19:06:40
SRV-NET-SUP-07	Success	18:27:30	18:28:37

Ici, on peut voir que la sauvegarde s'est effectuée correctement.

5.4 Conclusion du projet :

Dans ce projet, j'ai cherché à développer différentes compétences :

- Gérer le patrimoine informatique
- Répondre aux incidents et aux demandes d'assistance et d'évolution
- Travailler en mode projet
- Mettre à disposition des utilisateurs un service informatique

La migration des disques serveurs vers le format VHDX et leur centralisation sur les volumes réseau a été menée à bien pour l'ensemble des serveurs concernés. Grâce à une planification rigoureuse, à la coordination avec les équipes applicatives et à la mise en œuvre d'une procédure standardisée, chaque intervention a pu être effectuée dans les créneaux définis, avec un impact maîtrisé sur la production.

Cela a également permis de supprimer un job dans Veeam, puisque toutes les données seront sauvegardées par le même job.

Je n'ai rencontré aucune difficulté sur ce projet, mis à part pour obtenir des rendez-vous avec les chefs de projet en raison de leur planning chargé et de l'arrêt de l'application.

Toutes les opérations se sont déroulées avec succès : les sauvegardes Veeam ont été vérifiées en amont, les LUN iSCSI ont été convertis et réintégrés dans l'infrastructure Hyper-V via SCVMM, puis les services applicatifs ont été redémarrés et validés. Aucun incident n'a été constaté et aucune perte de données n'a été relevée.

Ce projet permet désormais de disposer d'une architecture unifiée, plus fiable et compatible avec l'arrivée des nouveaux serveurs Hyper-V 2025. Il constitue une étape importante dans la modernisation de l'infrastructure virtuelle et renforce la maintenabilité ainsi que la résilience du système d'information.

6 Projet Personnalisé Encadré n°2 : Installation d'un Serveur SFTP sous Oracle Linux 9.5

6.1 Contexte du Projet :

Suite à une demande de mise en production (MEP) un serveur dédié doit être mis en place afin de permettre des échanges de fichiers sécurisés.

Ce serveur sera déployé dans l'environnement virtuel existant basé sur Hyper-V et sera équipé d'une carte réseau positionnée en DMZ (zone démilitarisée), afin d'isoler et sécuriser les flux entrants et sortants.

Le serveur fonctionnera sous Oracle Linux 9.5, version choisie pour sa stabilité, son support à long terme et sa compatibilité avec les exigences de sécurité de l'organisation.

Le rôle principal de ce serveur sera d'héberger un service SFTP sécurisé (port 22) permettant à la plateforme PDI de se connecter et de déposer des fichiers au format JSON dans un répertoire.

Les fichiers déposés dans ce dossier seront récupérés via SFTP à l'aide du compte utilisateur SOWESIGN, configuré avec des droits d'accès strictement limités au répertoire de travail prévu.

Nous avons choisi de mettre en place un serveur SFTP plutôt qu'une solution FTPS, car cette dernière était plus complexe à configurer et moins adaptée à nos besoins.

6.2 Organisation et contraintes :

Infrastructure :

- Hyperviseur : Hyper-V (environnement existant).
- VM dédiée avec carte réseau en DMZ.
- Système d'exploitation : Oracle Linux 9.5.

Comptes et accès :

- Compte SFTP dédié.
- Accès autorisé uniquement depuis l'adresse IP de PDI.
- Accès limité au dossier /data.

Protocoles et ports :

- SFTP via SSH sur le port 22 et un accès en interne.

Ci-dessous le planning de déroulement de ce projet.

Serveur SFTP

DIAGRAMME DE GANTT

REGION Pays de la Loire
Chef de projet : Corentin CHAUVEL

TÂCHE	ATTRIBUÉE À	AVANCEMENT	DÉBUT	FIN	DUREE	Semaine d'affichage :							8 sept 2025					15 sept 2025						
						08/09/2025	1	8 sept 2025					8	9	10	11	12	13	14	15	16	17	18	19
Phase 1 - Préparation																								
Prise en compte de la MEP	Corentin CHAUVEL	100%	8/9/25	8/9/25	5																			
Phase 2 - Intervention technique																								
Mise en place	Corentin CHAUVEL	100%	8/9/25	8/9/25	12																			
Création de la VM sur l'hyperviseur	Corentin CHAUVEL	100%	8/9/25	8/9/25																				
Installation du système d'exploitation	Corentin CHAUVEL	100%	8/9/25	8/9/25	1h30																			
DNS	Corentin CHAUVEL	100%	8/9/25	8/9/25	40min																			
Paramétrage de la VM	Corentin CHAUVEL	100%	9/9/25	9/9/25	1h10																			
Configuration de la sauvegarde Veeam	Corentin CHAUVEL	100%	9/9/25	9/9/25	1h05																			
Configuration SFTP	Corentin CHAUVEL	100%	9/9/25	9/9/25	1h																			
Supprimer l'accès en SSH au compte root	Corentin CHAUVEL	100%	9/9/25	9/9/25	1h																			
Configuration Firewall	Corentin CHAUVEL	100%	10/9/25	10/9/25	1h30																			
Configuration DNS extérieur	Corentin CHAUVEL	100%	10/9/25	10/9/25	5min																			
Supervision dans Centreon	Corentin CHAUVEL	100%	10/9/25	10/9/25	1h																			
Phase 3 - Validation & Clôture																								
Vérification post-intervention	Corentin CHAUVEL	100%	12/9/25	12/9/25	1																			

Figure 13 : Gantt

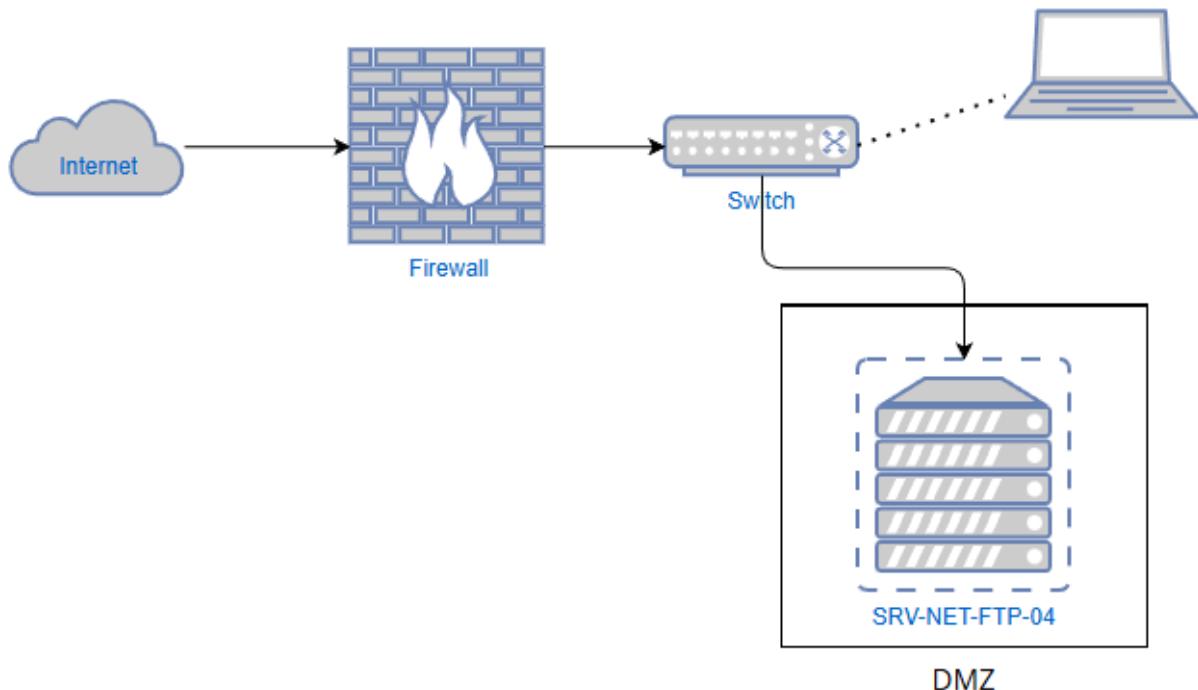


Figure 14 : Schéma simplifié du réseau pour le projet.

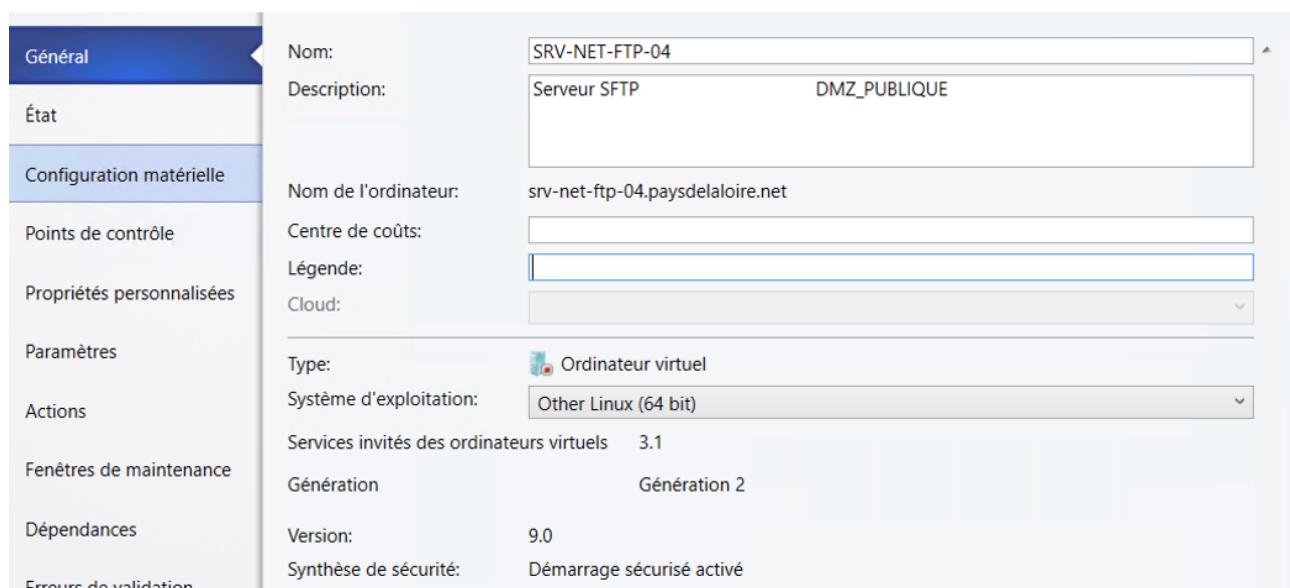
6.3 Créeation de la VM sur l'hyperviseur :

Dans un premier temps, je procède à la création de la machine virtuelle (VM) sur l'hyperviseur.

Pour cela, je me connecte à la console Virtual Machine Manager (VMM), qui permet d'administrer l'ensemble des VM hébergées sur les différents clusters Hyper-V.

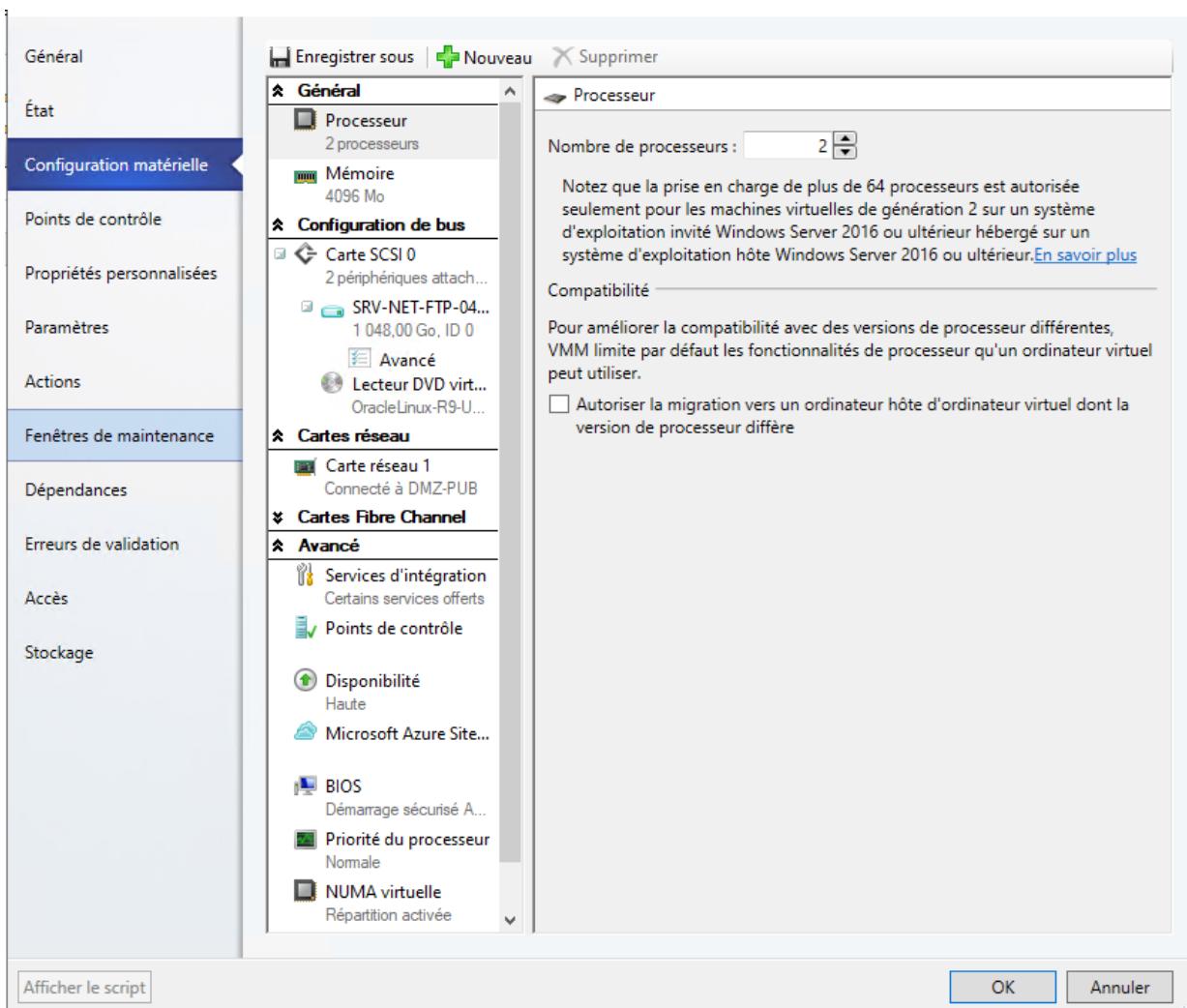
Depuis cette console, je lance l'assistant de création d'une nouvelle VM. Les premières étapes consistent à renseigner les paramètres de base :

- Nom de la VM
- Description
- Système d'exploitation invité (type et version)



Vient ensuite la configuration technique, où je définis les ressources en fonction des besoins exprimés dans la MEP (Mise en Production) :

- Nombre de processeurs virtuels (vCPU)
- Quantité de mémoire RAM
- Taille et type du disque dur virtuel (VHDX)
- Version de l'OS à installer
- Configuration de la ou des cartes réseau (DMZ)



Ensuite, je sélectionne l'hyperviseur hôte sur lequel sera déployée la VM, en privilégiant celui qui dispose du moins de charge (répartition équilibrée des VM).

Évaluation	Destination	Avertisse...	Type de transfe...	Optimisa...
★★★★★	SRV-NET-VIR-30.paysdelaloire.net	⚠ Réseau	✓	
★★★★★	SRV-S2D-VIR-02.paysdelaloire.net	⚠ Réseau	✓	
★★★★★	SRV-NET-VIR-31.paysdelaloire.net	⚠ Réseau	✓	
★★★★★	SRV-NET-VIR-37.paysdelaloire.net	⚠ Réseau		
★★★★★	SRV-NET-VIR-35.paysdelaloire.net	⚠ Réseau		
★★★★★	SRV-NET-VIR-36.paysdelaloire.net	⚠ Réseau		
★★★★★	SRV-NET-VIR-33.paysdelaloire.net	⚠ Réseau	✓	
★★★★★	SRV-NET-VIR-34.paysdelaloire.net	⚠ Réseau		

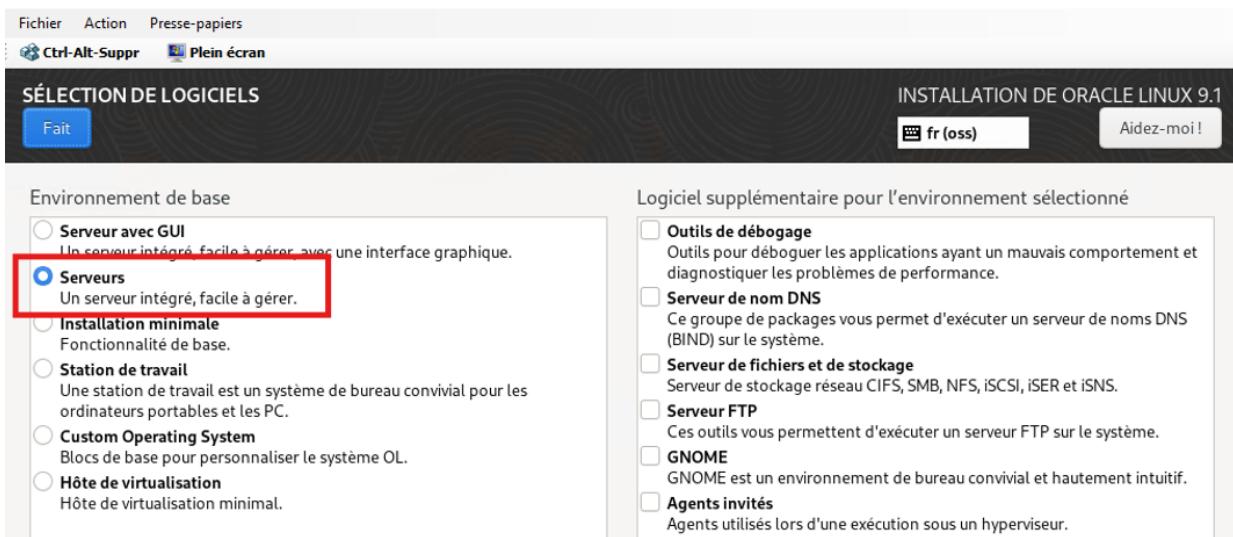
Enfin, je définis le stockage de la VM en choisissant le datastore disposant du plus d'espace disponible, afin d'assurer la redondance et la répartition de la charge.

6.4 Installation du système d'exploitation

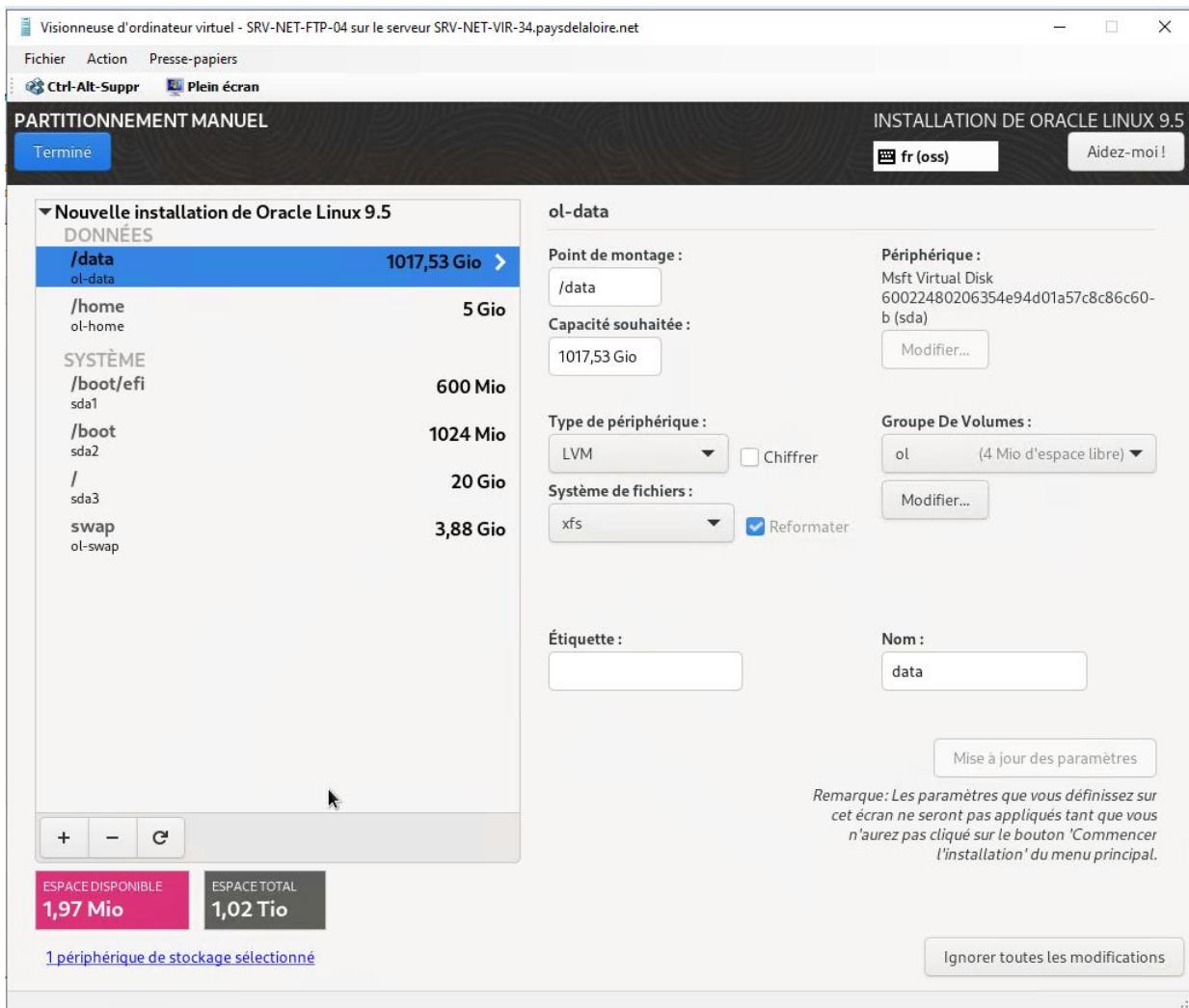
Une fois la VM créée, je procède au démarrage et à l'installation de l'OS via la console de la VM.

Dans ce cas, il s'agit d'une installation classique d'Oracle Linux 9.5.

Lors de la sélection des logiciels, je choisis le rôle Serveur minimal, car une interface graphique n'est pas nécessaire.



Je configure le partitionnement du disque, en créant notamment une partition /DATA d'une taille de 1017,53 Go, comme demandé.



Je configure la carte réseau en attribuant une adresse IP statique issue du plan d'adres-sage (dans la plage DMZ_Publique), en veillant à utiliser une adresse libre.

Modification de eth0 X

Nom de la connexion **eth0**

Général Ethernet Sécurité 802.1X DCB Proxy **Paramètres IPv4** Paramètres IPv6

Méthode **Manuel** ▾

Adresses

Adresse	Masque de réseau	Passerelle	
	24		Ajouter
			Supprimer

Serveurs DNS

Domaines de recherche

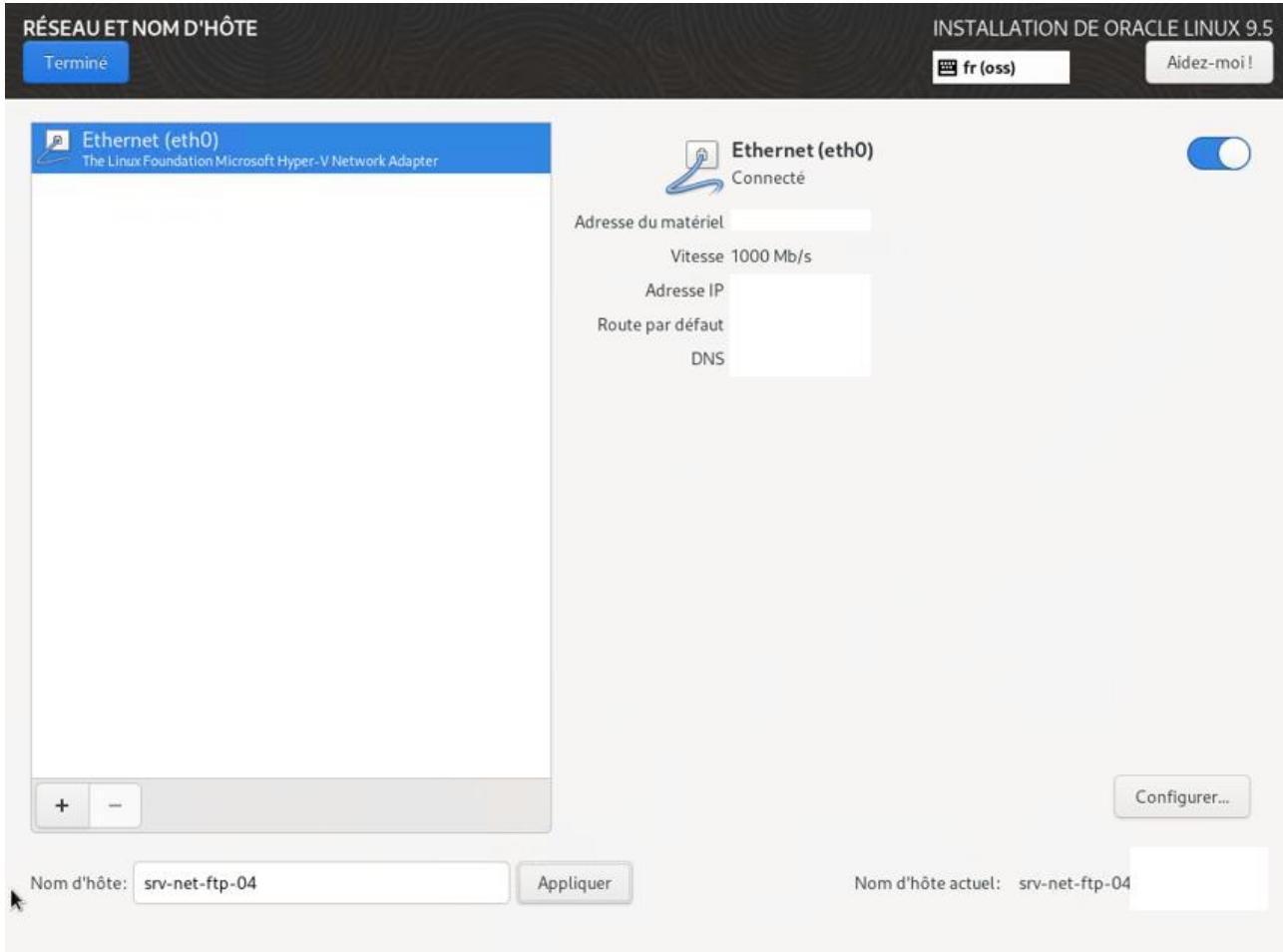
ID de client DHCP

Requiert un adressage IPv4 pour que cette connexion fonctionne

Routes...

Annuler **Enregistrer**

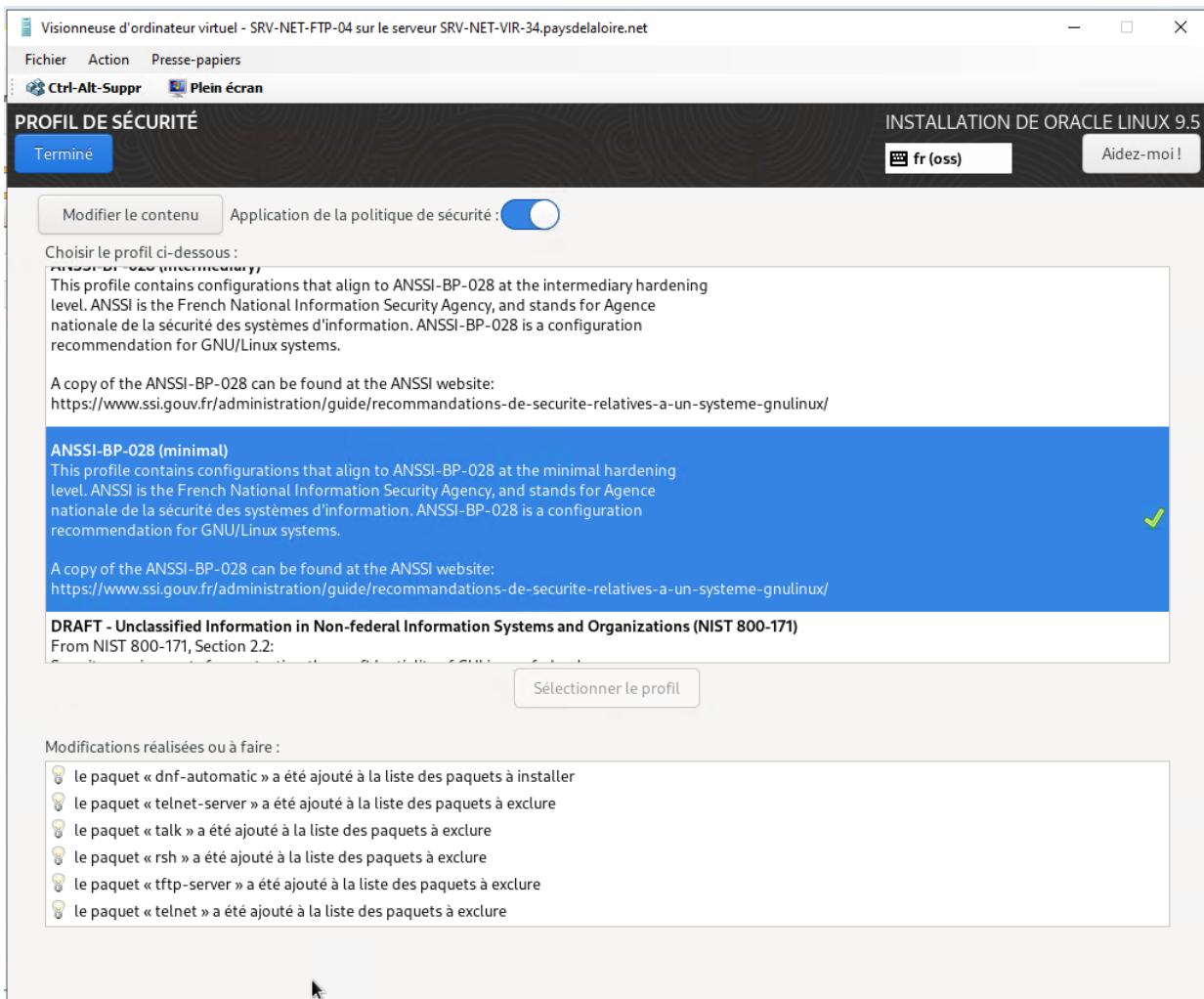
Je teste ensuite la connectivité réseau pour vérifier que la VM communique correctement et que l'adresse attribuée est bien fonctionnelle.



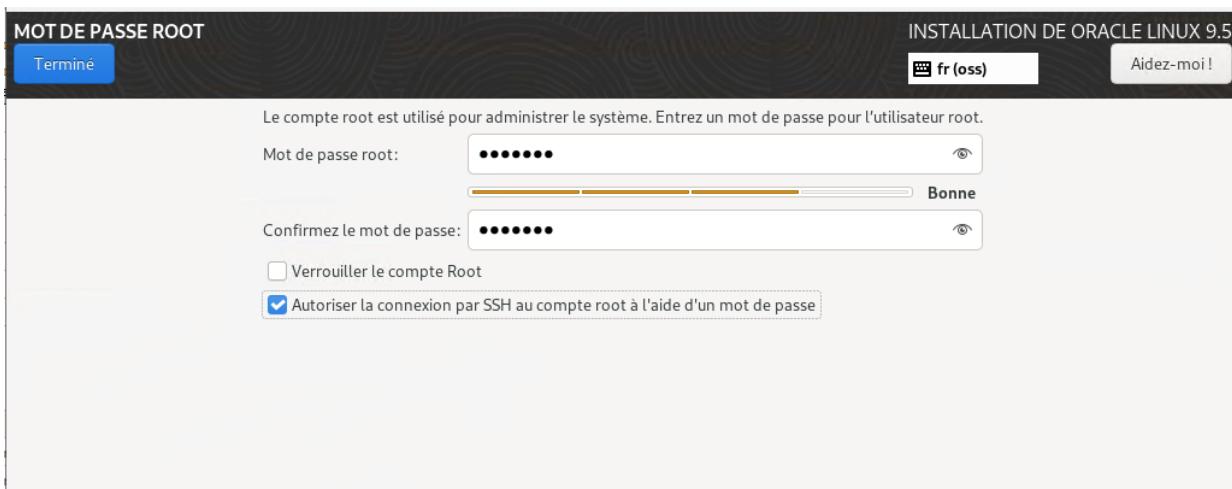
Je n'oublie pas de lui mettre un nom.

Sécurité et finalisation :

- Choix du profil de sécurité :
Je sélectionne le profil de sécurité ANSSI-BP-028 afin d'appliquer les recommandations.
- Je définis le mot de passe root conformément aux règles de sécurité en vigueur (complexité, longueur, expiration, etc.).



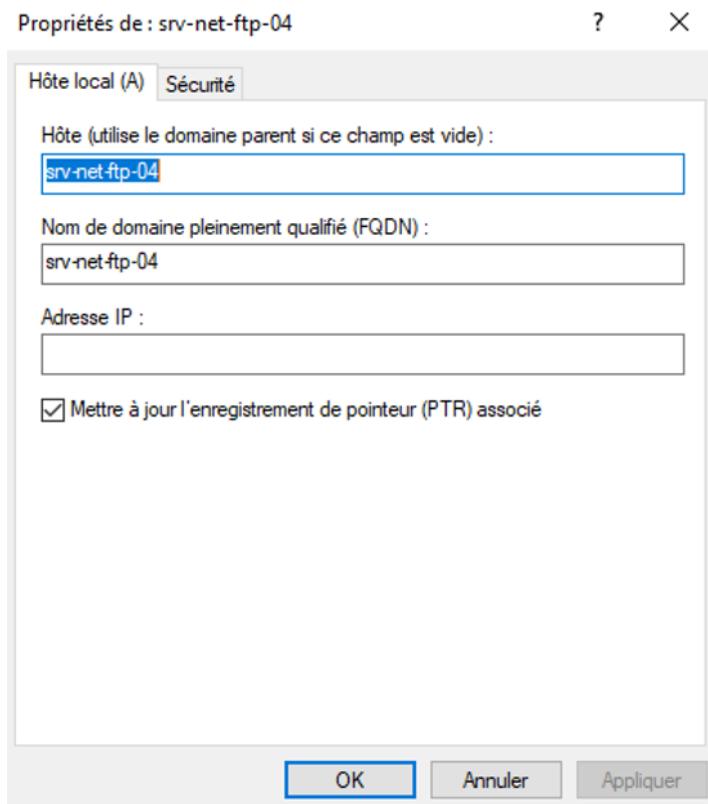
Configuration du MDP root et autorisation de la connections SSH le temps du déploiement :



Une fois tous ces paramètres saisis, je peux lancer l'installation.

6.5 DNS

Enfin, j'ajoute l'enregistrement DNS correspondant à la nouvelle VM, afin qu'elle soit correctement résolue sur le réseau.



6.6 Paramétrage de la VM :

Connexion en SSH a la machine pour pouvoir faire des copier-coller et pour être plus efficace.

6.6.1 Configuration SNMP :

Pour que l'on puisse superviser la VM depuis Centreon il faut configurer le SNMP (Simple Network Management Protocol) avec ces différentes commandes :

```
yum install net-snmp-utils.x86_64 net-snmp.x86_64      # Installe SNMP et ses outils.  
systemctl enable snmpd.service                         # Active le service SNMP au démarrage.  
systemctl start snmpd.service                          # Démarré le service SNMP.  
vi /etc/snmp/snmpd.conf                                # Ouvre le fichier de configuration SNMP  
pour modification.
```

Entrez la configuration requise. (Je ne peux pas la montrer pour des raisons de sécurité.)

6.6.2 Désinstallation de Firewalld :

On désinstalle le firewalld car nous préférons utiliser IPTABLES.

```
systemctl stop firewalld    # Stoppe le pare-feu.
```

```
systemctl disable firewalld      # Désactive le démarrage auto du pare-feu.  
systemctl mask --now firewalld # Bloque totalement le pare-feu et l'arrête.
```

Voici pourquoi on utilise Iptables, il offre un contrôle très fin sur la configuration du pare-feu, permettant d'ajuster chaque règle exactement comme on le souhaite. Cette précision le rend particulièrement adapté aux configurations complexes. Son fonctionnement reste entièrement prédictible, puisque les règles sont exécutées dans un ordre strict et linéaire, ce qui facilite la compréhension pour les administrateurs habitués à ce modèle. Comme il ne repose sur aucune couche d'abstraction, iptables donne une maîtrise directe du filtrage réseau.

6.6.3 Installation de IPTABLES :

```
yum install iptables-services          # Installe le service iptables.  
systemctl start iptables               # Démarrer iptables.  
systemctl enable iptables              # Active iptables au démarrage.  
systemctl status iptables              # Affiche l'état d'iptables.
```

6.6.4 Configuration de IPTABLES :

```
mkdir /home/root # Crée le répertoire /home/root.
```

Copie du script de configuration du firewall (créer auparavant avec des règles spéciales pour cette VM) dans /home/root : fw-dmz-srv-net-ftp-04.sh

Pour exécuter le script (la configuration a été masquée pour des raisons de confidentialités):

```
sh ./fw-dmz-srv-net-ftp-04.sh
```

Pour voir les logs iptables : *vi /etc/sysconfig/iptables*

```
service iptables save      # Sauvegarde les règles iptables actuelles.  
service iptables restart    # Redémarre le service iptables.  
iptables -nvL --line-numbers  # Affiche les règles iptables avec détails et numéros de ligne.
```

6.6.5 Mise à jour :

```
dnf update -y      # Met à jour tous les paquets sans demander de confirmation.  
dnf upgrade -y    # Met à niveau tous les paquets installés sans demander de confirmation.
```

6.6.6 Déploiement de l'antivirus avec Ansible :

Ansible est un outil open source qui sert à automatiser la gestion des serveurs et l'installation de logiciels. Il ne nécessite pas d'agent sur les machines : il se connecte simplement via SSH. Les actions à réaliser sont décrites dans des fichiers lisibles appelés playbooks (en YAML).

Grâce à son fonctionnement fiable et répétable, Ansible permet de déployer rapidement des applications, configurer plusieurs serveurs en même temps et éviter les erreurs humaines. C'est un outil simple, efficace et très utilisé pour automatiser l'infrastructure informatique.

Se connecter sur le serveur Ansible avec le compte root.

Editer le fichier :

```
vi /etc/ansible/inventory.ini
```

Le fichier inventory.ini sert à indiquer à Ansible sur quelles machines exécuter ses tâches.

Et ajouter la section :

```
[S-ONE-FTP]  
SRV-NET-FTP-04
```

Ensuite éditer :

```
vi /etc/ansible/playbooks/deploy_sentinelone_agent.yaml
```

```
- #hosts: tests  
  hosts: S-ONE-MDM  
  name: Install SentinelOne Linux agent  
  vars:
```

Modifier hosts en : S-ONE-FTP

C'est le script qui permet de déployer l'antivirus.

Déployer la clé SSH de la vm ansible vers la vm cible :

```
ssh-copy-id SRV-NET-FTP-04
```

Faire le déploiement de l'antivirus :

```
cd /etc/ansible
```

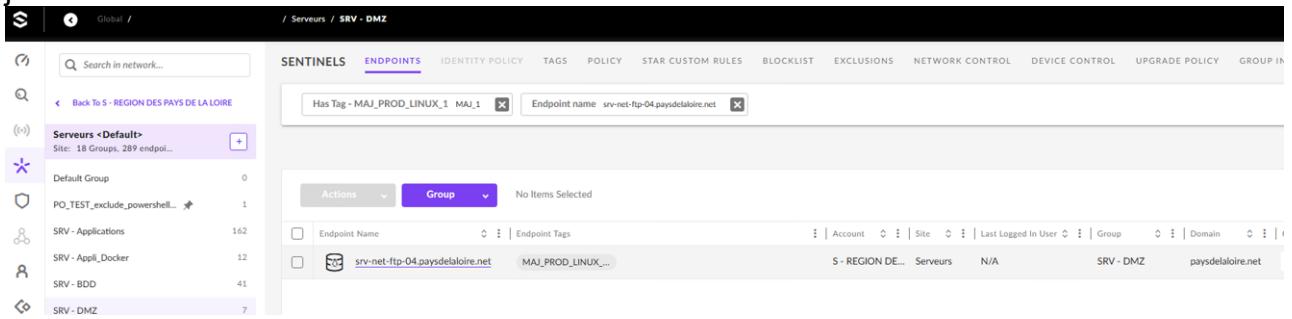
```
ansible S-ONE-FTP -m ping -i inventory.ini      # Teste la connexion Ansible avec le  
groupe d'hôtes S-ONE-FTP défini dans inventory.ini.
```

Installation du playbook :

```
cd /etc/ansible/playbooks      # Va dans le dossier contenant les playbooks Ansible.  
ansible-playbook deploy_sentinelone_agent.yaml  # Exécute le deploy_sentinelone_agent.yaml.
```

Et l'antivirus est déployé.

Sur la console de l'antivirus déplacer la VM dans le bon groupe (SRV-DMZ)
Et ajouter le TAG « MAJ_PROD_LINUX_1 », cela permet de les repérer lors des mises à jour.



The screenshot shows the Sophos Endpoint Management interface. The top navigation bar includes 'Global', 'Servers / SRV - DMZ', and various policy and control tabs. On the left, a sidebar lists groups: 'Default Group' (0), 'PO_TEST_exclude_powershell...' (1), 'SRV - Applications' (162), 'SRV - Appli_Docker' (12), 'SRV - BDD' (41), and 'SRV - DMZ' (7). The main content area is titled 'SENTINELS' and shows an 'ENDPOINTS' search bar with filters 'Has Tag - MAJ_PROD_LINUX_1 MAJ_1' and 'Endpoint name srv-net-ftp-04.paysdelaloire.net'. Below this, a table lists endpoints with columns: Actions, Group (set to 'Group'), Endpoint Name, Endpoint Tags, Account, Site, Last Logged In User, Group, Domain, and Site. One endpoint is listed: 'srv-net-ftp-04.paysdelaloire.net' with tag 'MAJ_PROD_LINUX_1', grouped under 'SRV - DMZ'.

6.6.7 Déploiement de la page d'accueil :

```
cd /etc/ansible/playbooks      # Va dans le dossier contenant les playbooks d'Ansible.
```

```
vi copy_BANNER_Shell.yaml      # Edit le fichier
```

modifier la ligne :

```
hosts : S-ONE-FTP
```

```
ansible-playbook copy_BANNER_Shell.yaml  # Exécute le ansible-playbook copy_BANNER_Shell.yaml.
```

REGION PHYS DE LA LOIRE

```
*****  
*      !! ACCES sous CONTROLE !!      *  
*      -----      *  
*  Toute tentative de connexion sans      *  
* AUTORISATION préalable est interdite *  
*      et possible de POURSUITES !!      *  
*      --      *  
*      UNAUTHORIZED ACCESS PROHIBITED      *  
*****
```

```
SRV-NET-FTP-04  >  Serveur linux SFTP en DMZ publique
```

```
computer-vm  
Operating System : Oracle Linux Server 9.5  
Install Date: mer. 19 mars 2025 14:46:07
```

```
Sys. de fichiers Taille Utilisé Dispo Utile Monté sur  
/dev/sda3      20G      3,4G    17G  17% /
```

	total	used	free	shared	buff/cache	available
Mem:	3,3Gi	1,4Gi	768Mi	15Mi	1,4Gi	1,9Gi
Swap:	3,9Gi	0B	3,9Gi			

```
Last login : exploita pts/0 10.244.0.225 Wed Sep 10 10:43 still logged in
```

```
Time      Last Reboot      Connected      Charge du système à 1, 5, 15 minutes  
10:43:57 up 1 day, 23:41, 2 users, load average: 0,00, 0,00, 0,00
```

MERCI DE NE PAS STOCKER DE FICHIERS SUR LES SERVEURS

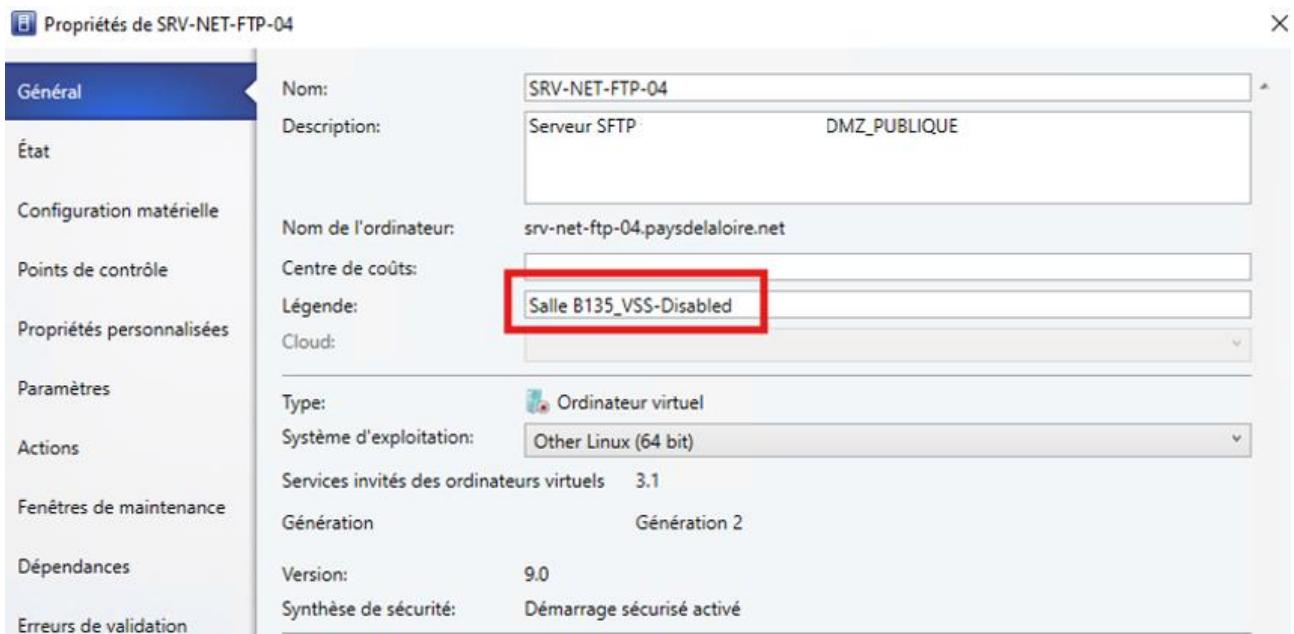
```
[exploitation@srv-net-ftp-04 ~]$ █
```

Cette page d'accueil permet d'obtenir directement des informations essentielles sur la machine.

6.7 Configuration de la sauvegarde Veeam :

Mise à jour du champ Légende : Salle B135_VSS-Disabled

On rajoute ce champ dans la légende pour que Veeam répartisse la charge entre les proxys Veeam pour la sauvegarde entre les deux salles.



6.8 Configuration SFTP :

Créer un utilisateur pour SFTP :

```
useradd -m sowesign      # Crée un utilisateur sowesign avec un répertoire personnel.
passwd sowesign          # Définit ou modifie le mot de passe de l'utilisateur sowesign.
```

Configurer SSH pour SFTP et le répertoire /data :

Nous allons maintenant configurer le serveur SSH pour qu'il utilise le répertoire /data comme emplacement des fichiers pour le serveur SFTP et restreindre l'accès uniquement à SFTP (en interdisant l'accès SSH classique).

Modifier la configuration de SSH (/etc/ssh/sshd_config) :
Ouvrir le fichier de configuration SSH avec un éditeur de texte :

```
vi /etc/ssh/sshd_config    # Ouvre le fichier de configuration du serveur SSH pour édition.
```

Restreindre l'utilisateur sowesign à un répertoire spécifique et uniquement SFTP avec c'est différente commande :

```
Match User sowesign        # Applique les règles suivantes uniquement à l'utilisateur sowesign.
ChrootDirectory /data       # Restreint l'utilisateur à l'arborescence /data.
ForceCommand internal-sftp  # Force l'usage uniquement du service SFTP (pas de shell).
AllowTcpForwarding no       # Désactive le transfert TCP pour cet utilisateur.
```

Configurer les répertoires et les permissions :

Maintenant, que le répertoire /data existe et que les permissions sont correctement définies.

```
mkdir -p /data/sowesign # Crée le dossier /data/sowesign
```

Définir les bonnes permissions :

S'assurer que le répertoire /data possède les bonnes permissions pour permettre à l'utilisateur sowesign d'y accéder de manière sécurisée. Le répertoire parent /data doit appartenir à root, tandis que le répertoire de l'utilisateur doit appartenir à l'utilisateur lui-même.

Répertoire parent /data doit être possédé par root :

```
chown root:root /data # Définit root comme propriétaire et groupe de /data.  
chmod 755 /data # Donne les droits lecture/execute à tous et écriture au propriétaire sur /data.
```

Répertoire utilisateur /data/sowesign doit être possédé par sowesign :

```
chown sowesign:sowesign /data/sowesign # Attribue la propriété de /data/sowesign à l'utilisateur et groupe sowesign.  
chmod 700 /data/sowesign # Donne tous les droits au propriétaire sowesign uniquement.
```

Redémarrage du service SSH pour que les modifications prennent effet :

```
systemctl restart sshd
```

Tester la connexion SFTP :

Essayez maintenant de vous connecter au serveur SFTP en utilisant un client SFTP.

```
sftp sowesign@0.0.0.0
```

6.9 Supprimer l'accès en SSH au compte root :

Bloquer l'accès root en SSH/SFTP limite les risques d'intrusion et protège le serveur en forçant l'utilisation de comptes utilisateurs sécurisés avant toute administration.

Création d'un compte exploitation pour pouvoir se connecter en ssh :

Avec c'est commande :

```
useradd exploitation # Crée l'utilisateur exploitation.  
passwd exploitation # Définit ou change le mot de passe de exploitation.
```

Se placer dans le répertoire `/etc/ssh/sshd_config.d/` puis éditer le fichier `01-permitrootlogin.conf` avec la commande `vi` et remplacer `PermitRootLogin yes` par `PermitRootLogin no`.

```
# This file has been generated by the Anaconda Installer.  
# Allow root to log in using ssh. Remove this file to opt-out.  
PermitRootLogin no
```

Ensuite éditer le fichier `/etc/ssh/sshd_config` avec la commande `vi` et remplacer `PermitRootLogin prohibit-password` par `PermitRootLogin no`

```
# If you want to change the port on a SELinux system, you have to tell
# SELinux about this change.
# semanage port -a -t ssh_port_t -p tcp #PORTNUMBER
#
#Port 22
#AddressFamily any
#ListenAddress 0.0.0.0
#ListenAddress ::

#HostKey /etc/ssh/ssh_host_rsa_key
#HostKey /etc/ssh/ssh_host_ecdsa_key
#HostKey /etc/ssh/ssh_host_ed25519_key

# Ciphers and keying
#RekeyLimit default none

# Logging
#SyslogFacility AUTH
#LogLevel INFO

# Authentication:

#LoginGraceTime 2m
PermitRootLogin no
#StrictModes yes
#MaxAuthTries 6
#MaxAuthtries 6
```

Redémarrer le service sshd avec la commande : `systemctl restart sshd.service`

Je vérifie ensuite si root a des clés SSH valides :

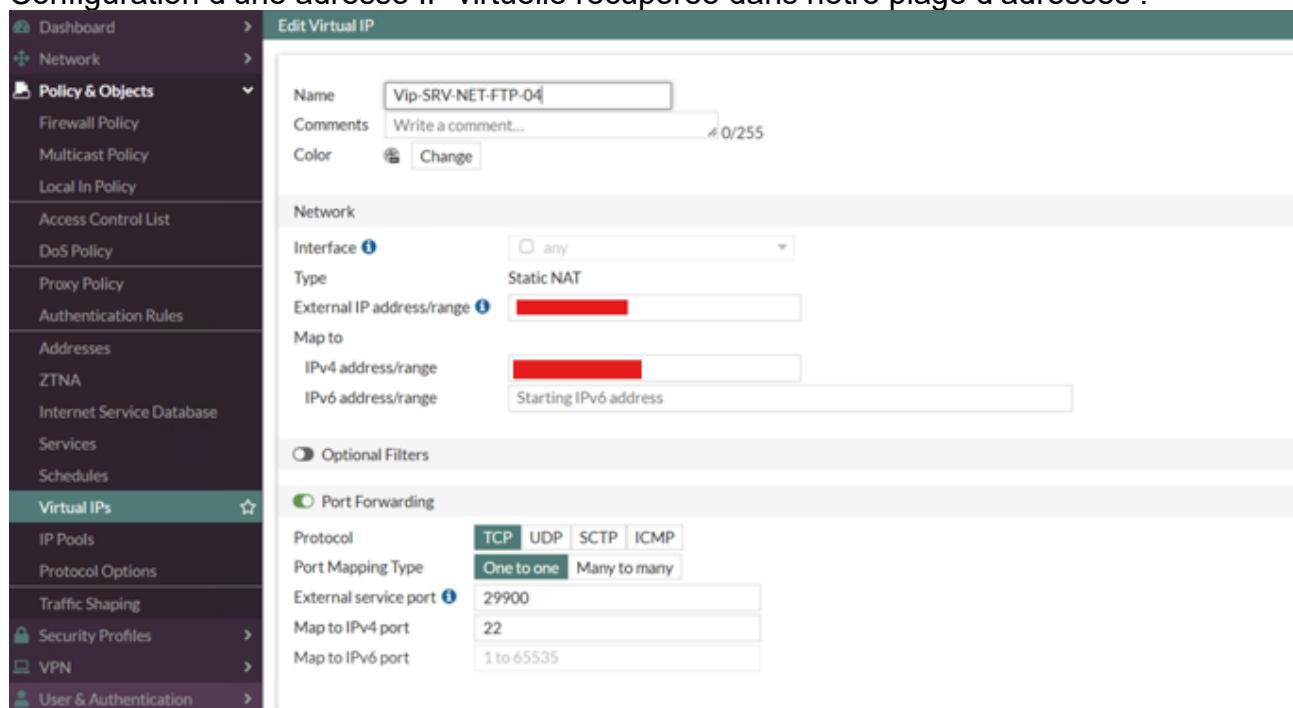
`ls -l /root/.ssh/authorized_keys`

Si ce fichier existe et contient une clé publique, alors root peut toujours se connecter. Pour bloquer cela, supprimez le fichier avec cette commande :

`rm -f /root/.ssh/authorized_keys`

6.10 Configuration du Firewall :

Configuration d'une adresse IP virtuelle récupérée dans notre plage d'adresses :



The screenshot shows a 'Virtual IPs' configuration screen. The 'Edit Virtual IP' dialog is open for a policy named 'Vip-SRV-NET-FTP-04'. The 'Network' section is set to 'Static NAT' with 'any' interface. The 'External IP address/range' and 'Map to' fields are redacted. The 'Optional Filters' section has a 'Port Forwarding' tab selected. Under 'Protocol', 'TCP' is selected. Under 'Port Mapping Type', 'One to one' is selected. The 'External service port' is set to '29900', 'Map to IPv4 port' is '22', and 'Map to IPv6 port' is '1 to 65535'.

Ensuite configuration des règles :



Z-LAN → Z-DMZ_PUBLIC											
acces SFTP	[REDACTED]	[REDACTED]	[REDACTED]	always	ssh ALL_ICMP	✓ ACCEPT		Disabled	Standard		
accès serveur SFTP	[REDACTED]	[REDACTED]	[REDACTED]	always	TCP_29900	✓ ACCEPT		Disabled	Standard		
	[REDACTED]	[REDACTED]	[REDACTED]	always	ssh HTTP	✓ ACCEPT		Disabled	Standard		
Z-WAN → Z-DMZ_PUBLIC											
[REDACTED]				always		ALL		✓ ACCEPT		Disabled	Standard

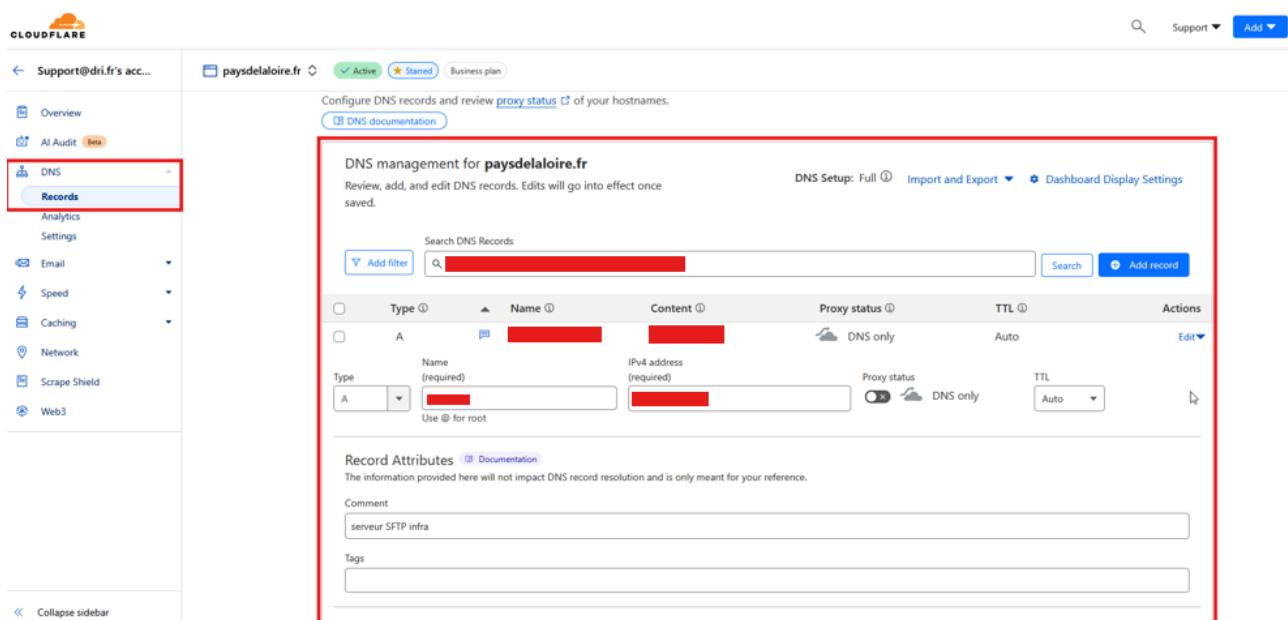
Je configure une règle de pare-feu du LAN vers la DMZ pour autoriser les connexions SSH et ICMP depuis les réseaux internes. L'accès au service SFTP est également autorisé depuis le LAN via le port TCP 29900. De plus, le serveur Ansible est autorisé à communiquer avec le serveur pour l'orchestration et la gestion automatisée.

Pour le WAN vers la DMZ, je crée une règle permettant uniquement l'accès depuis l'adresse IP publique du serveur, renforçant ainsi la sécurité en limitant l'exposition externe.

6.11 Configuration DNS extérieur :

Cloudflare est une entreprise américaine qui propose des services liés à la sécurité, à la performance et à la fiabilité des sites web et des applications en ligne. L'un de ses services les plus connus est le DNS public, qui permet de gérer les enregistrements DNS (Domain Name System) de votre domaine.

Sur Cloudflare voici la configuration DNS extérieur qu'il faut mettre en place :



Cloudflare

Support@drif.fr's acc... Active Starred Business plan

Overview AI Audit Beta

DNS Records Analytics Settings

Email Speed Caching Network Scrape Shield Web3

Collapse sidebar

Support Add

Configure DNS records and review proxy status of your hostnames. DNS documentation

DNS management for paysdelaloire.fr DNS Setup: Full Import and Export Dashboard Display Settings

Review, add, and edit DNS records. Edits will go into effect once saved.

Add filter Search DNS Records Search Add record

Type	Name	Content	Proxy status	TTL	Actions
A	[REDACTED]	[REDACTED]	DNS only	Auto	Edit

Type: A, Name: [REDACTED], Content: [REDACTED], Proxy status: DNS only, TTL: Auto

Record Attributes Documentation
The information provided here will not impact DNS record resolution and is only meant for your reference.

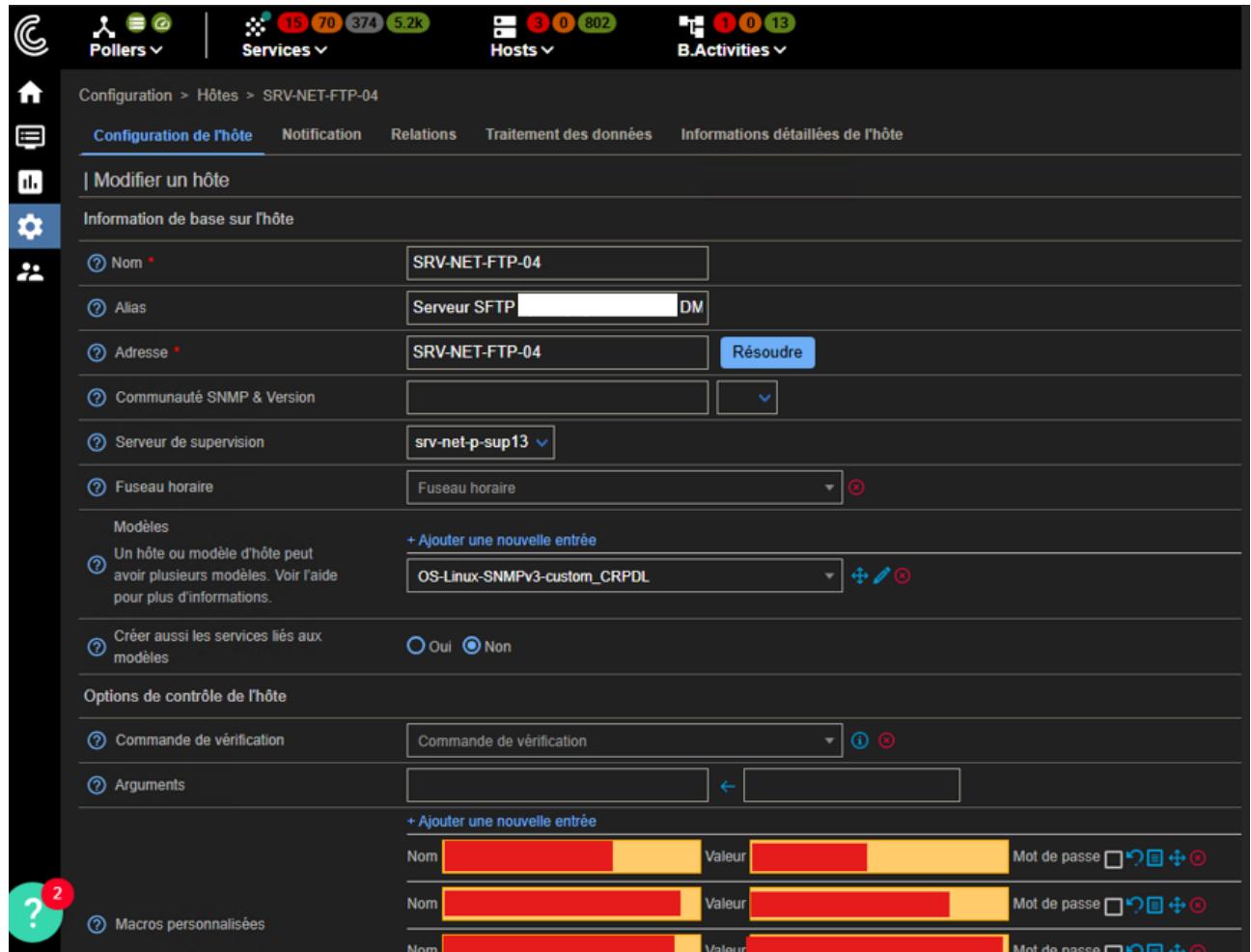
Comment: serveur SFTP infra

Tags:

Créer une entrée DNS avec l'adresse IP et le nom, il n'y a pas plus de configuration.

6.12 Paramétrage de la supervision dans Centreon

Une fois sur l'outil de supervision, je me dirige dans l'onglet Configuration > Hôtes > Hôtes. Je recherche ensuite un serveur FTP pour pouvoir dupliquer ça configuration. Et je modifie avec mes besoins :



The screenshot shows the Centreon host configuration interface for the host 'SRV-NET-FTP-04'. The configuration page includes the following fields:

- Information de base sur l'hôte**
 - Nom**: SRV-NET-FTP-04
 - Alias**: Serveur SFTP DM
 - Adresse**: SRV-NET-FTP-04
 - Communauté SNMP & Version**: (empty)
 - Serveur de supervision**: srv-net-p-sup13
 - Fuseau horaire**: Fuseau horaire
- Modèles**
 - Un hôte ou modèle d'hôte peut avoir plusieurs modèles. Voir l'aide pour plus d'informations.
 - Ajouter une nouvelle entrée**: OS-Linux-SNMPV3-custom_CRPDL
- Créer aussi les services liés aux modèles**: Oui Non
- Options de contrôle de l'hôte**
 - Commande de vérification**: Commande de vérification
 - Arguments**: (empty)
 - Ajouter une nouvelle entrée**: (empty)
 - Macros personnalisées**: (empty)

Et pour finir j'enregistre la configuration et je l'exporte vers les deux serveurs Centreon.

Explication du fonctionnement de la supervision avec le SNMPV3 : La supervision d'un serveur Linux avec Centreon en SNMPV3 repose sur une communication sécurisée entre Centreon et l'agent SNMP du serveur (SNMPD). Centreon envoie des requêtes SNMPV3 contenant un utilisateur, un mot de passe d'authentification et un mot de passe de chiffrement. Le serveur Linux vérifie ces informations, puis renvoie les données système (CPU, mémoire, disque, réseau). Centreon interprète ensuite ces valeurs et les affiche dans l'interface sous forme d'alertes et de graphiques.

6.13 Conclusion :

Dans ce projet, j'ai cherché à développer différentes compétences :

- Gérer le patrimoine informatique
- Répondre aux incidents et aux demandes d'assistance et d'évolution
- Travailler en mode projet
- Mettre à disposition des utilisateurs un service informatique

La mise en place de ce serveur dédié répond efficacement aux besoins de la mise en production en offrant une solution sécurisée pour les échanges de fichiers. Intégré dans l'infrastructure virtuelle existante sous Hyper-V et positionné en DMZ, il garantit une isolation optimale des flux réseaux tout en respectant les exigences de sécurité de l'organisation.

Grâce à l'utilisation d'Oracle Linux 9.5, le serveur bénéficie d'un environnement stable, fiable et adapté aux contraintes de production. Le service SFTP, configuré spécifiquement pour le compte soweesign avec des droits strictement limités, assure un transfert de fichiers sécurisé.

Je n'ai rencontré aucune difficulté sur ce projet. J'ai également sensibilisé les collaborateurs afin qu'ils évitent de déposer n'importe quel fichier sur le serveur et qu'ils ne diffusent pas le mot de passe.

Ce projet permet ainsi d'assurer des échanges de données contrôlés, protégés et conformes aux bonnes pratiques.

Les améliorations qui pourraient être fait par la suite la mise en place de l'authentification par clés SSH, l'utilisateur possède une clé privée, tandis que le serveur stocke la clé publique correspondante. Lors de la connexion, le serveur vérifie que les deux clés s'associent correctement, ce qui permet d'accéder sans utiliser de mot de passe.

Ce système est beaucoup plus sécurisé qu'un mot de passe classique : il est quasiment impossible à brute-forcer, seules les personnes disposant de la clé privée peuvent se connecter.

7 Portfolio / Site entreprise

Pour illustrer mon parcours et présenter mes réalisations, j'ai conçu un portfolio en ligne, accessible à l'adresse suivante : <https://corentin.chauvel.formation-esiac.fr/>

La conception de ce portfolio m'a permis d'organiser mon développement professionnel en mettant en valeur les compétences que j'ai acquises ainsi que les expériences réalisées au sein de l'entreprise. J'ai également pu développer la présence en ligne de l'organisation en créant le site web de notre entreprise pédagogique. Voici le lien : <http://ntxsystem.fr/>

Sur le site web on trouve aussi le lien des portfolios de mes collègues avec qui j'ai confectonné ce site.

8 Conclusion générale

Cette période d'alternance m'a offert une expérience particulièrement enrichissante, tant sur le plan professionnel que personnel. En intégrant le service informatique, j'ai pu découvrir le fonctionnement concret d'une infrastructure système et réseau au sein d'un environnement professionnel exigeant. J'ai eu l'occasion de participer activement à diverses missions telles que la surveillance et l'exploitation des infrastructures, l'installation et la gestion de serveurs physiques et virtuels, l'intégration et la maintenance d'équipements réseau, ainsi que la résolution de tickets d'incidents.

Ces activités parmi d'autres m'ont permis de consolider mes compétences techniques, d'approfondir mes connaissances en administration système et réseau, et de me familiariser avec des outils et technologies récents. Au-delà des aspects purement techniques, cette expérience m'a également permis de développer mon autonomie, mon sens des responsabilités.

Fort de cette expérience, je souhaite poursuivre mes études au sein de l'ENI avec un BAC+4 Administrateur Système et Réseau, afin de continuer à développer mes compétences dans le domaine de l'administration des systèmes, des réseaux et de la cybersécurité.

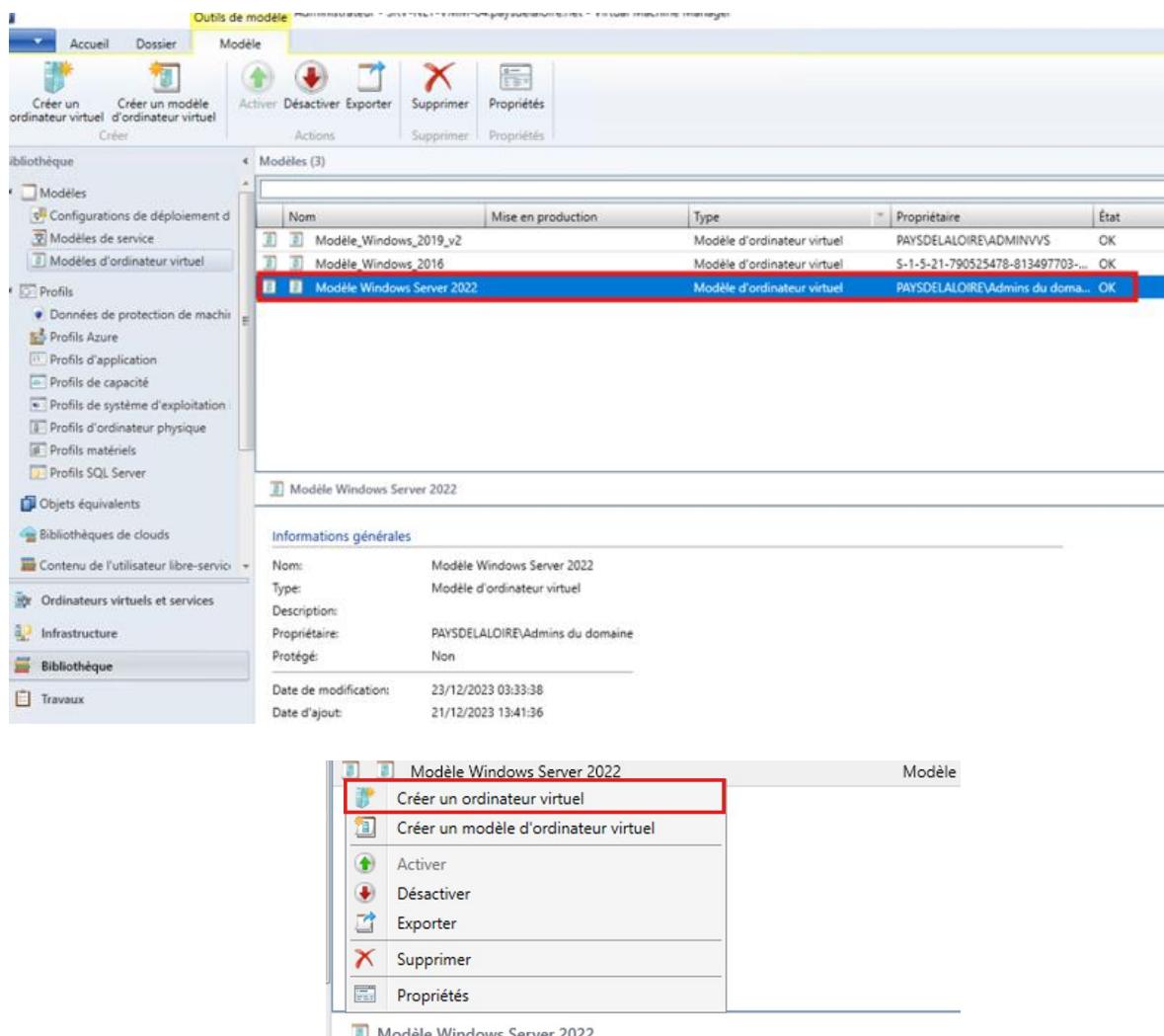
En somme, cette alternance a constitué une étape déterminante dans mon parcours. Elle m'a permis de gagner en autonomie, en confiance et en expertise, tout en confirmant ma volonté d'évoluer dans le secteur des technologies de l'information.

9 ANNEXES

9.1 Annexe 1 : Procédure d'Installation d'une VM Windows

CREATION DE LA VM DANS SCVMM (System Center Virtual Machine Manager)

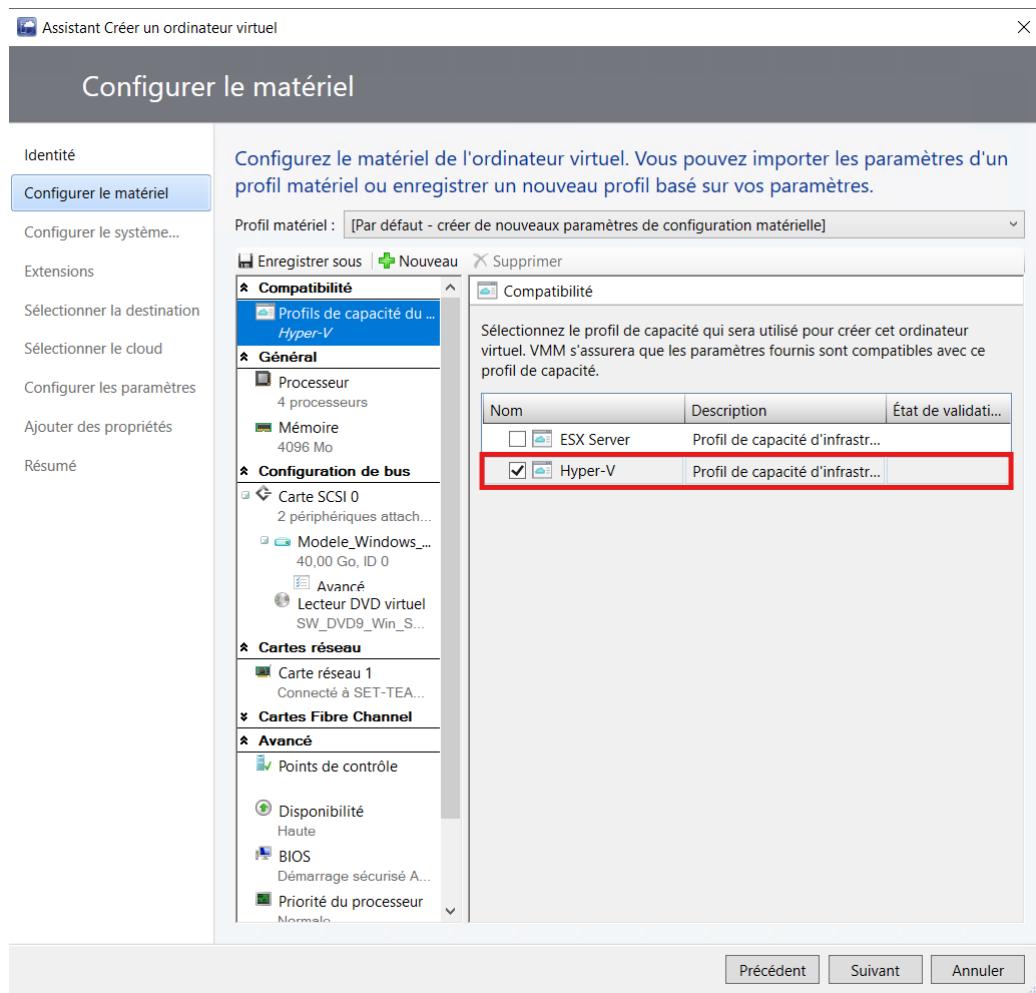
Se rendre sur le SRV-NET-VMM-04 : ouvrir la Console Virtual Machine Manager
Créer la VM à l'aide d'un modèle.



Renseigner le nom de la machine ainsi qu'une courte description.

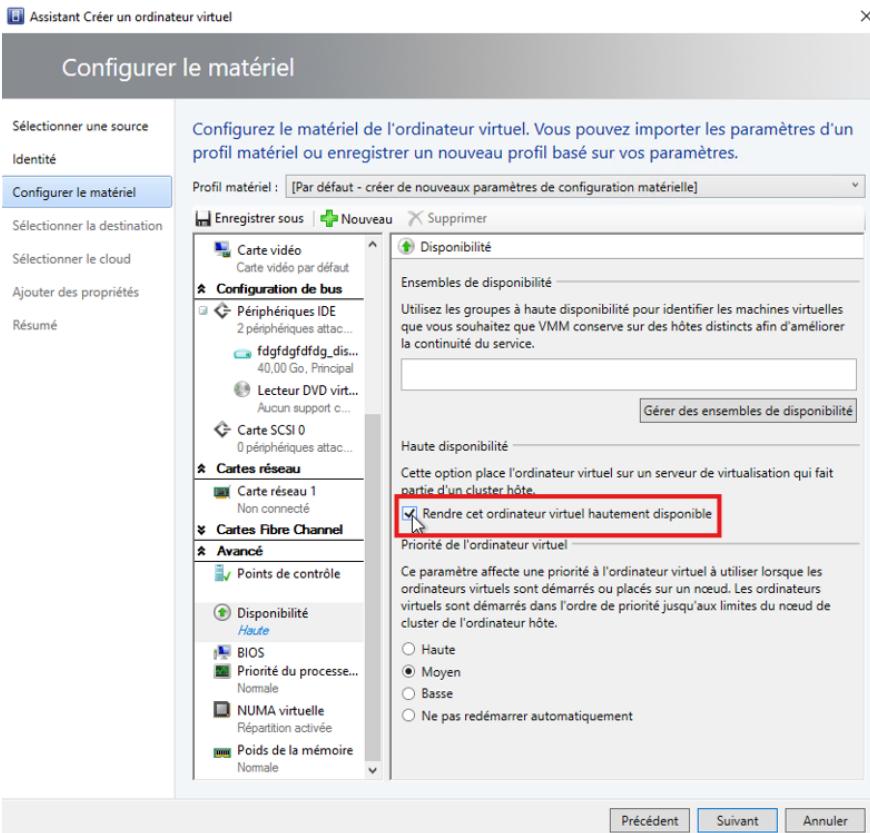


Sélectionner Hyper-V dans la section Compatibilité, puisque nos hyperviseurs sont basés sur Hyper-V.

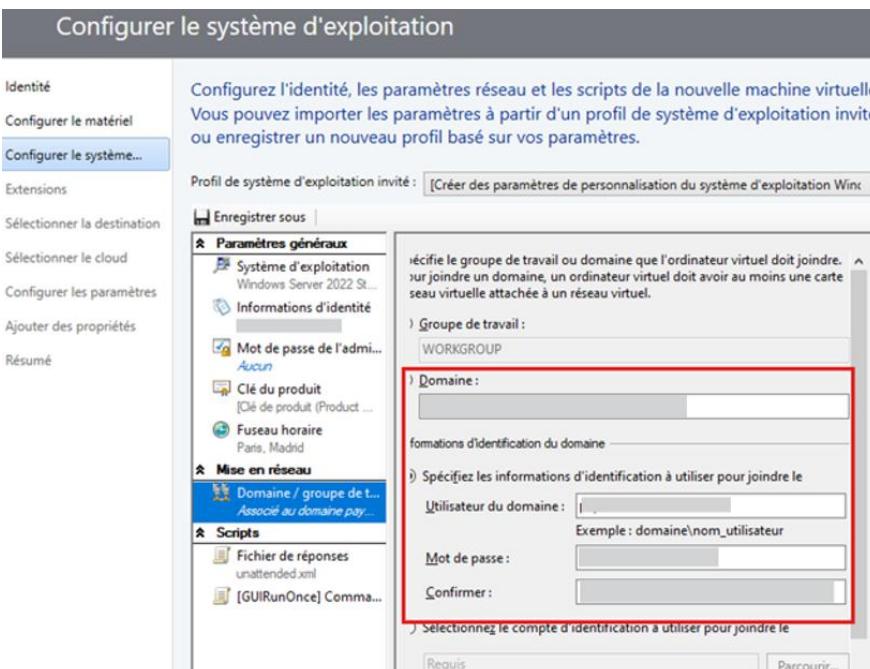


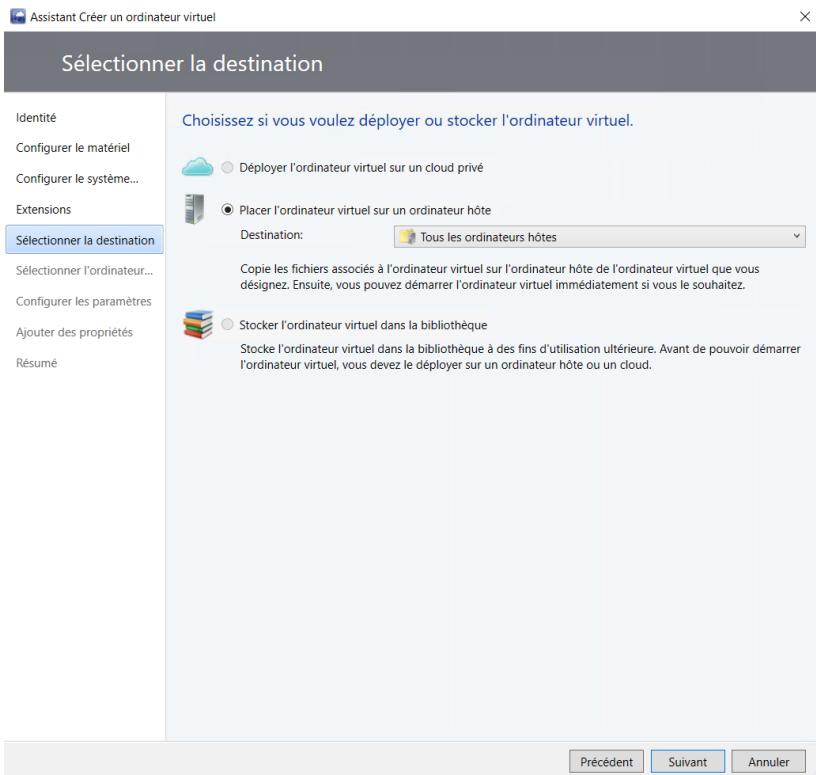
Choisir ensuite le nombre de processeurs, la quantité de mémoire RAM, ainsi que l'espace disque à allouer au second disque, si nécessaire. La carte réseau est déjà configurée par défaut sur le réseau LAN.

Activer l'option permettant de rendre l'ordinateur hautement disponible.

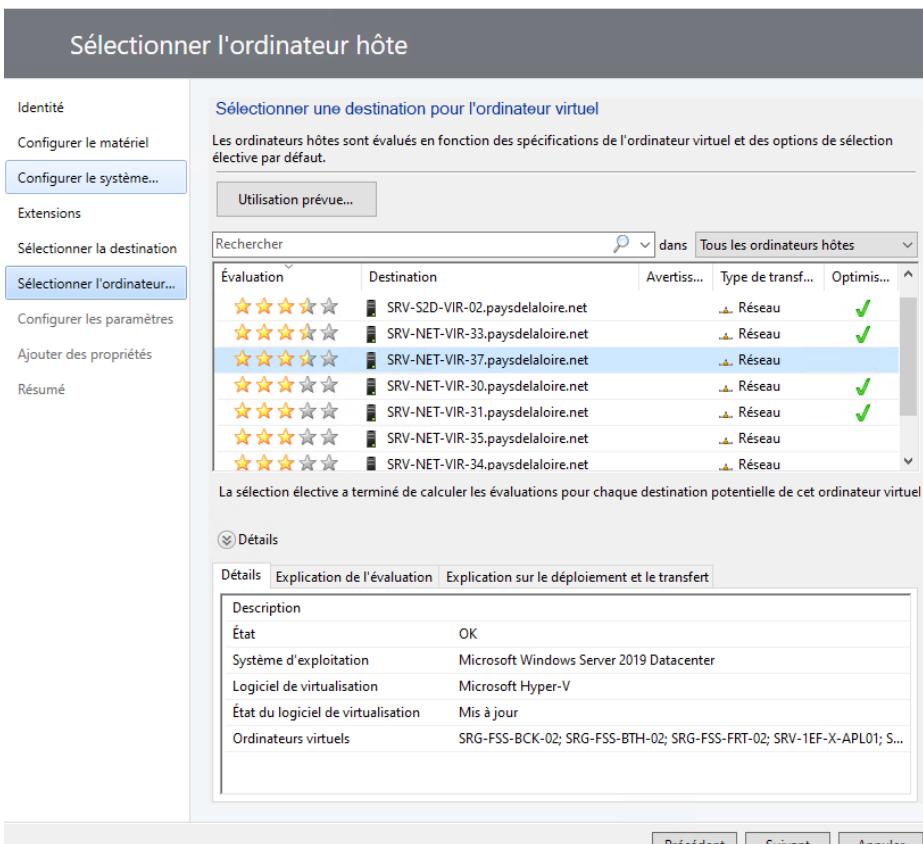


Indiquer le nom de domaine afin que la machine l'intègre automatiquement.





Placer la VM sur l'un des hyperviseurs recommandés.



Configurer les paramètres

Identité
Configurer le matériel
Configurer le système...
Extensions
Sélectionner la destination
Sélectionner l'ordinateur...
Configurer les paramètres
Ajouter des propriétés
Résumé

Vérifier les paramètres de l'ordinateur virtuel

Les valeurs suivantes seront utilisées lors de la création d'un ordinateur virtuel :

Emplacements
Emplacement de l'ordinateur virtuel : C:\ClusterStorage\Volume20\Modèle Win2022_disque_1.vhdx

Paramètres du système d'exploitation
Informations d'identité : SRV-1EF-P-APL01

Mise en réseau
Carte réseau 0 : SET-TEAM01

Fibre Channel

Ressources de l'ordinateur
Disque dur virtuel : Modèle Win2022_disque_1.vhdx

Ressource de bibliothèque : Modèle Win2022_disque_C
Taille du fichier : 16,21 Go

Options de déploiement : Méthode de déploiement du disque dur virtuel sur l'ordinateur hôte : Transférer le disque dur virtuel à l'aide du réseau

Détails du déploiement :
Source : \\SRV-NET-VMM-04.paysde...
Chemin de destination : C:\ClusterStorage\Volume20\Modèle Win2022_disque_1.vhdx
Nom de fichier : Modèle Win2022_disque_1.vhdx

Si on déploie un modèle, il faut modifier le nom du fichier (nom du serveur_disque_1.vhdx)

Ajouter des propriétés

Identité
Configurer le matériel
Configurer le système...
Extensions
Sélectionner la destination
Sélectionner l'ordinateur...
Configurer les paramètres
Ajouter des propriétés
Résumé

Actions automatiques : Sélectionner une action à exécuter automatiquement lors du démarrage du serveur de virtualisation :

Ne pas activer l'ordinateur virtuel

Démarrage retardé (secondes) : 0

Action lors de l'arrêt du serveur de virtualisation :

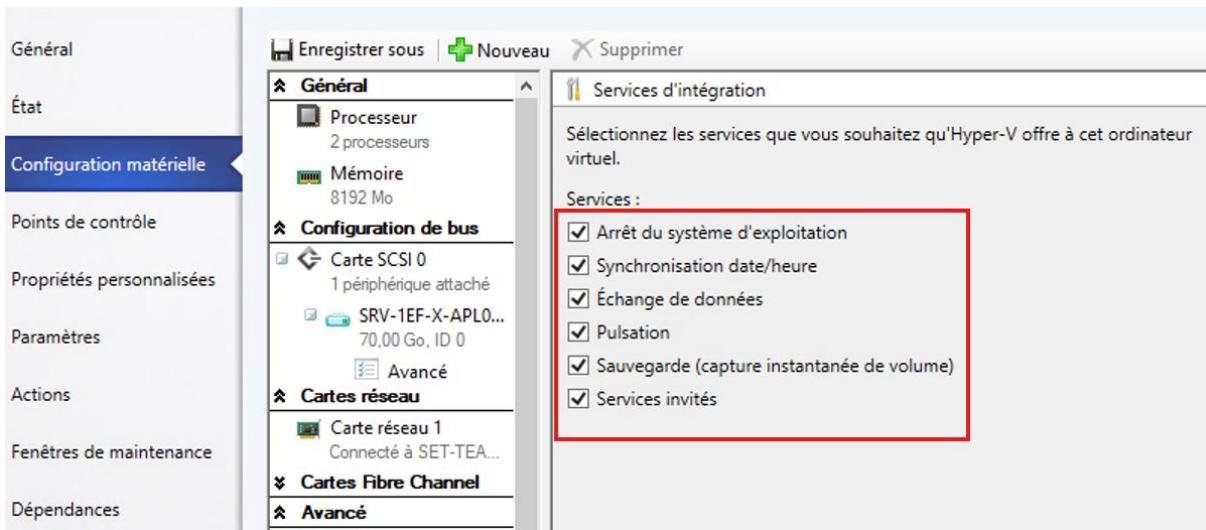
Enregistrer l'état

Optimisation des performances et des ressources (PRO) : Utilisez cette option pour empêcher l'optimisation dynamique ou PRO de migrer l'ordinateur virtuel.

Exclure l'ordinateur virtuel des actions d'optimisation

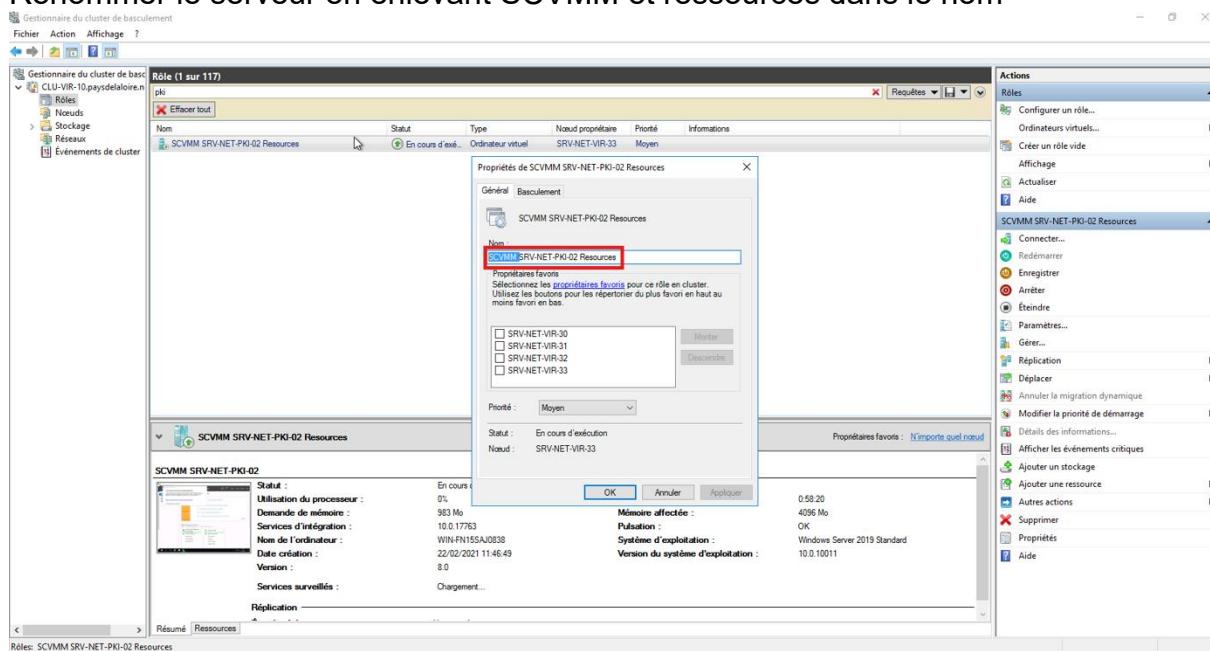
A faire après la création :

Vérifier que tous les services d'intégration sont cochés, y compris Services invités.



POST-INSTALLATION

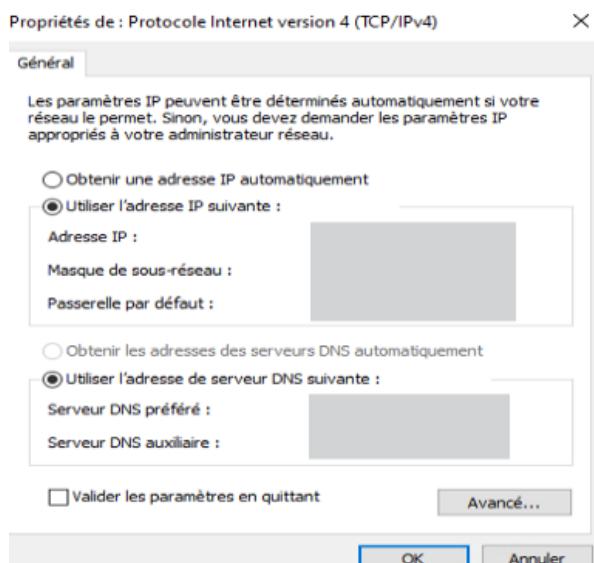
Se connecter sur le srv-net-vir-XX qui héberge la VM, lancer le logiciel « gestionnaire du cluster de basculement », rechercher le serveur et clic droit propriétés. Renommer le serveur en enlevant SCVMM et ressources dans le nom



Se connecter en utilisant la console VMM avec le mot de passe du compte administrateur local créé dans le keepass.

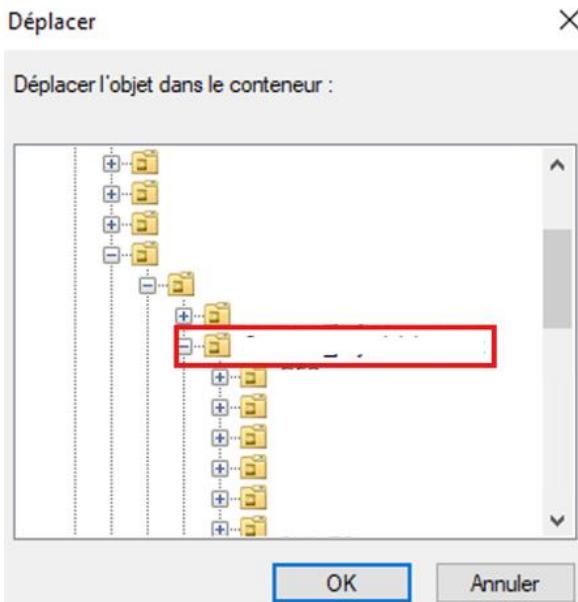


Mettre un IP fixe en fonction du plan d'adressage.



Renommer le nom du serveur

Une fois l'opération effectuée et avant le redémarrage, déplacez le compte d'ordinateur dans la bonne OU.



Installation Utilitaires

Ajout du client SCCM

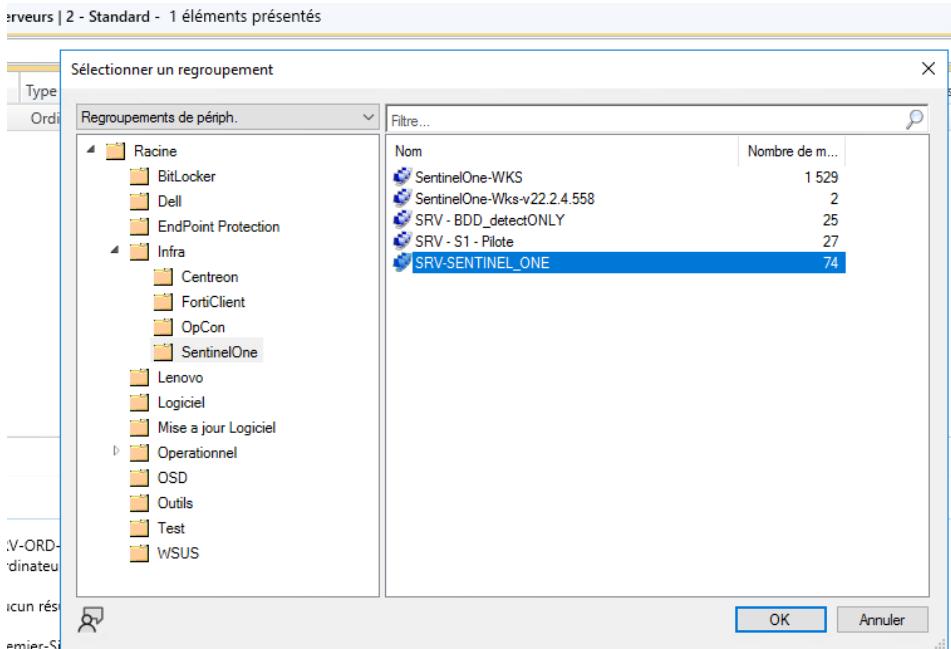
Avec cette ligne de commande. (Ligne de commande cachée.)

Une fois le client installé sur le serveur, il faut mettre le serveur dans le bon groupe dans SCCM pour le déploiement des mises à jour.

Icone	Nom	Limitation au regroupement	Nombre de membres	Membres visibles sur le site	Regroupements référencés
WSUS_Global	Tous les clients poste de travail	1 446	1 446	2	
WSUS_Pilotes	Tous les clients poste de travail	74	74	0	
WSUS_SERVERS	Windows Server 2016	1	1	3	
WSUS_Serveurs 1 - Pilotes	Servers All	31	31	2	
WSUS_Serveurs 2 - Standard	Servers All	127	127	4	
WSUS_Serveurs 3 - Critique	Servers All	17	17	1	
WSUS_Serveurs 4 - Manuel	Servers All	39	39	0	

Ensuite :

Vérification de l'installation de S1 (Antivirus)
 Déplacer le serveur dans le groupe correspondant à son usage.



Mises à jour Windows :

Intégrer le serveur dans la sauvegarde Veeam

Tagger les VM dans SCVMM, les Tags sont à ajouter pour chaque VM dans :

Propriétés > Légende

Il faut tagger les VM en fonction des Hyper-V qui les héberge, il s'agit simplement d'une répartition de charge entre les proxys Veeam qui sont en B135 ou D009 :

Configuration WALLIX Bastion :

WALLIX Bastion est une solution de PAM (Privileged Access Management), c'est-à-dire une solution de gestion des accès à priviléges. Elle permet de sécuriser, contrôler et tracer les accès des utilisateurs (internes ou externes) aux systèmes informatiques sensibles d'une entreprise.

C'est un outil essentiel pour renforcer la cybersécurité dans les organisations, notamment dans les environnements où plusieurs administrateurs, prestataires ou techniciens accèdent à des systèmes critiques.

Ajout dans le Bastion :

Renseigner le nom du serveur, son adresse IP, puis ajouter le service RDP et sélectionner le service correspondant.

The screenshot shows two main parts of the WALLIX Bastion web interface.

Left Side (Equipment List):

- Header: **Équipements**
- Actions: **Ajouter** (Add)
- Table Headers: **Nom**, **Adresse IP ou FQDN**, **Dernière connexion**, **Services**, **Étiquettes**
- Table Data (List of targets):

	Nom	Adresse IP ou FQDN	Dernière connexion	Services	Étiquettes
1			2024-03-18 11:36:17	RDP-PRESTA	-
2			2024-03-18 11:38:58	RDP-PRESTA	-
3			2024-03-18 11:41:16	RDP-PRESTA, (+1)	-
4			-	RDP-PRESTA	-
5			2024-06-18 11:44:34	RDP-PRESTA	-
6			-	RDP-PRESTA	-
7			2024-06-18 11:44:12	RDP-PRESTA	-
8			2024-01-19 13:43:56	RDP-PRESTA	-
9			2024-06-18 11:44:08	RDP-PRESTA	-
10			-	RDP-PRESTA	-
11			2024-05-31 18:19:42	RDP-PRESTA	-
12			2023-12-15 16:15:27	RDP-PRESTA	-
13			2024-08-20 10:41:03	RDP-PRESTA	-
14			-	RDP-PRESTA	-
15			-	RDP-PRESTA	-
16			-	RDP-PRESTA	-

Left Sidebar:

- Tableaux de bord
- Mes autorisations
- Audit
- Utilisateurs
- Cibles** (highlighted)
- Équipements** (highlighted)
- Applications
- Domaines
- Comptes
- Clusters
- Groupes
- Plugins de coffres-forts
- Politiques d'emprunt
- Auto-Découverte
- Autorisations

Right Side (General Configuration):

- Header: **Général**
- Form Fields:
 - Nom*** (Name):
 - Alias**:
 - Adresse IP ou FQDN *** (IP or FQDN):
 - Description**:
- Buttons: **Valider** (Validate)
- Table Headers: **Général**, **Services**, **Domaines locaux**, **Comptes locaux**, **Groupes**, **Certificats**, **Étiquettes**
- Table Data (Status):

	Statut
1	Créé manuellement

Général Services D

+ Ajouter ▾

RDP

VNC

SSH

RLOGIN

TELNET

RAWTCPIP

TA

Modification du service RDP-PRESTA

X

Équipement

Nom de service

RDP-PRESTA

Port *

3389

Politique de connexion *

RDP-PRESTA

Domaine global

Un domaine global est obligatoire pour créer des cibles pour des applications et des clusters

Options proxy

RDP_CLIPBOARD_UP
 RDP_CLIPBOARD_DOWN
 RDP_CLIPBOARD_FILE
 RDP_PRINTER
 RDP_COM_PORT
 RDP_DRIVE
 RDP_SMARTCARD
 RDP_AUDIO_OUTPUT
 RDP_AUDIO_INPUT

FortiGate :

Création de la machine dans le FortiGate afin qu'elle puisse être accessible via le bastion.

The screenshot shows the Juniper Network Manager interface. The left sidebar is the navigation menu with the following structure:

- Dashboard
- Network
- Policy & Objects
 - Firewall Policy
 - Multicast Policy
 - IPv6 Multicast Policy
 - IPv4 Access Control List
 - IPv6 Access Control List
 - IPv4 DoS Policy
 - IPv6 DoS Policy
 - Proxy Policy
 - Authentication Rules
 - Addresses
 - ZTNA
 - Internet Service Database

The 'Addresses' option in the 'Policy & Objects' menu is highlighted with a red box. The main content area shows a list of addresses. A context menu is open over the 'Address' option in the list, with 'Create New' highlighted. The 'Edit Address' dialog is open, showing fields for Name, FQDN, and Interface. The entire 'Edit Address' dialog is highlighted with a red box.

Ajouter la machine dans le groupe GRP-VPNSSL-TSE (groupe d'accès au bastion)

The screenshot shows the Juniper Network Manager interface. The left sidebar is the navigation menu with the following structure:

- Dashboard
- Network
- Policy & Objects
 - Firewall Policy
 - Multicast Policy
 - IPv6 Multicast Policy
 - IPv4 Access Control List
 - IPv6 Access Control List
 - IPv4 DoS Policy
 - IPv6 DoS Policy
 - Proxy Policy
 - Authentication Rules
 - Addresses
 - ZTNA
 - Internet Service Database
 - Services
 - Schedules
 - Virtual IPs
 - IP Pools
 - Protocol Options
 - Traffic Shaping

The 'Addresses' option in the 'Policy & Objects' menu is highlighted with a red box. The main content area shows a list of address groups. A context menu is open over the 'Address Group' option in the list, with 'Create New' highlighted. The 'Edit Address Group' dialog is open, showing a list of address groups. The 'GRP-VPNSSL-TSE' group is highlighted with a red box.

9.2 Annexe 2 : Photo baie

