Documentation Technique - Projet Infrastructure ITWay

David Paul
Marseille Johan

Introduction

Le présent document constitue la documentation technique détaillée du projet d'infrastructure informatique mis en place pour ITWay, une entreprise spécialisée dans les services informatiques avec des bureaux à Marseille et Lille. Ce projet s'inscrit dans le cadre de l'amélioration continue des capacités de gestion et de sécurité des systèmes informatiques internes de l'entreprise, afin de répondre efficacement aux besoins croissants de ses clients en matière de disponibilité, de performance et de sécurité. Cette documentation couvre en détail l'ensemble des aspects techniques mis en œuvre : de l'architecture physique et virtuelle, jusqu'à la gestion proactive de la sécurité et de la continuité des activités. Le projet ITWay vise non seulement à moderniser l'infrastructure existante mais également à poser des bases solides pour une exploitation simplifiée et sécurisée à long terme.

Présentation d'ITWay

Historique

Créée en 2005, ITWay était initialement une petite société de conseil en informatique. Face à l'évolution rapide des besoins en services numériques et à la complexification des infrastructures IT, l'entreprise a progressivement étendu ses compétences. Dès 2018, elle ouvre une antenne régionale à Lille pour mieux répondre aux attentes de ses clients nationaux et internationaux.

Chiffres clés

- Nombre d'employés : 110 employés (80 à Marseille, 30 à Lille)
- Chiffre d'affaires annuel : 15 millions d'euros
- Clients : principalement des PME, mais aussi quelques grands comptes et administrations publiques

Organisation interne

Siège social (Marseille)

- Département IT (administration des systèmes, réseaux, sécurité) : 20 personnes
- Département développement logiciel : 15 personnes
- Support technique : 15 personnes
- Services administratifs (RH, finance, direction générale) : 20 personnes
- Commercial : 10 personnes

Antenne régionale (Lille)

- Support technique : 10 personnes
- Développement logiciel : 10 personnes
- Commercial : 10 personnes

Objectifs du projet

Sécurisation

Assurer la sécurité des données et des accès grâce à des solutions robustes telles que des VPN, DMZ, Radius et des mécanismes de détection d’intrusion et prévention proactive.

Innovation

Intégrer des technologies innovantes comme la virtualisation avec Proxmox, l'automatisation via Ansible et le monitoring avancé avec Grafana et Nagios, pour améliorer continuellement l'efficacité opérationnelle.

Simplification

Mettre en place des solutions faciles à exploiter et à administrer, réduisant ainsi la complexité du quotidien des équipes IT tout en augmentant leur réactivité face aux besoins internes et externes.

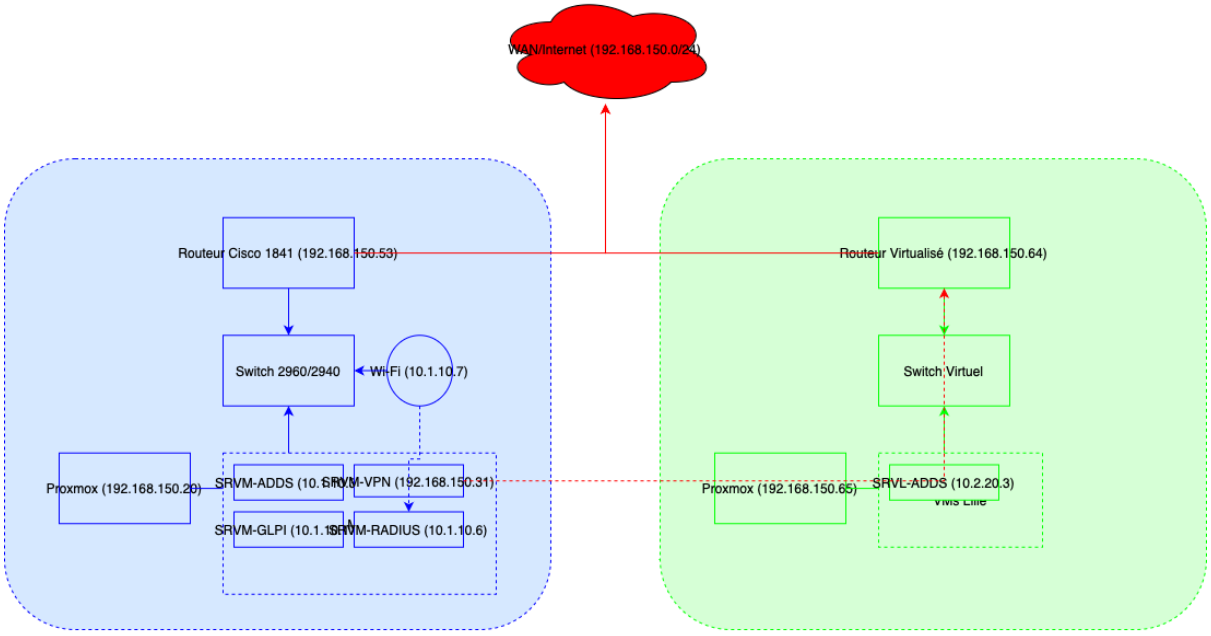
Architecture générale

Schéma réseau global

L'infrastructure ITWay repose sur un réseau WAN simulé par le réseau local de la salle de cours (192.168.150.0/24).

- **Marseille** : Routeur Cisco physique
- **Lille** : Routeur virtualisé (technologie au choix)
- **Hyperviseur** : Adresse IP fixe dédiée
- **Carte iLO** : Adresse IP fixe pour la gestion à distance

Schéma simplifié :



Légende: Bleu=Marseille, Vert=Lille, Rouge=WAN/VPN, Pointillés=Logique

- Marseille : VLANs pour serveurs, DMZ, Wi-Fi, utilisateurs
- Lille : VLANs similaires avec interconnexion via VPN
- Connexion WAN : 192.168.150.0/24

5. Convention de nommage

Une convention claire est adoptée pour faciliter la gestion :

- **Serveurs Marseille** : SRVM-XXX (ex. SRVM-ADDS)
- **Serveurs Lille** : SRVL-XXX (ex. SRVL-DHCP)
- **VLANs Marseille** : VLNM-XXX (ex. VLNM-010)
- **VLANs Lille** : VLNL-XXX (ex. VLNL-090)
- **Ordinateurs** : PC-XX-XX (ex. PC-010-01 : VLAN 010, poste 01)

6. Plan d'adressage IP

Le plan d'adressage est structuré pour segmenter les réseaux :

VLAN	Description	Site	Plage d'adresses	Masque	Passerelle
VLNM-010	Serveurs Internes	Marseille	10.1.10.0/24	255.255.255.0	10.1.10.1
VLNM-020	DMZ	Marseille	172.16.20.0/24	255.255.255.0	172.16.20.1
VLNM-030	Wi-Fi Interne	Marseille	192.168.30.0/27	255.255.255.224	192.168.30.1
VLNM-040	Utilisateurs Commercial	Marseille	192.168.40.0/28	255.255.255.240	192.168.40.1
VLNM-050	Utilisateurs IT	Marseille	192.168.50.0/27	255.255.255.224	192.168.50.1
VLNM-060	Services administratifs	Marseille	192.168.60.0/27	255.255.255.224	192.168.60.1
VLNM-070	Support technique	Marseille	192.168.70.0/27	255.255.255.224	192.168.70.1
VLNM-080	Développement	Marseille	192.168.80.0/27	255.255.255.224	192.168.80.1
VLNL-090	Serveurs Internes	Lille	10.2.20.0/24	255.255.255.0	10.2.20.1
VLNL-100	DMZ	Lille	172.16.100.0/24	255.255.255.0	172.16.100.1
VLNL-110	Wi-Fi Interne	Lille	192.168.110.0/27	255.255.255.224	192.168.110.1

VLNL-120	Utilisateurs Commercial	Lille	192.168.120.0/28	255.255.255.240	192.168.120.1
VLNL-130	Développement	Lille	192.168.130.0/28	255.255.255.240	192.168.130.1
VLNL-140	Support technique	Lille	192.168.140.0/28	255.255.255.240	192.168.140.1

7. Équipements physiques

Serveur physique (Marseille)

- **Numéro de série** : CZ201804W
- **DNS** : ILOCZ2018048W
- **Utilisateur** : Administrator
- **Mot de passe** : Y7R5FGC9
- **IP** : 192.168.150.42
- **Disques** : 6 (2x600 Go en RAID 1, 4x1,2 To en RAID 5)
- **RAM** : 64 Go

Routeur (Marseille)

- **Modèle** : Cisco 1841
- **IP** : 192.168.150.53
- **Connexion SSH** : ssh -oHostKeyAlgorithms=+ssh-rsa -oKexAlgorithms=+diffie-hellman-group1-sha1 -oCiphers=aes128-cbc,3des-cbc,aes192-cbc,aes256-cbc grp9@192.168.150.53
- **Mot de passe** : Uog6k02Cq

Switch (Marseille)

- **Modèle** : Cisco 2960/2940
- **Connexion** : sudo screen /dev/ttyUSB0
- **Mot de passe** : MRHac3p6D

Routeur (Lille)

- **IP** : 192.168.150.64
- **Utilisateur** : admin
- **Mot de passe** : pesqez-xynna3

8. Hyperviseur et virtualisation

Proxmox

- **Adresse** : https://192.168.150.20:8006/
- **Utilisateur** : root
- **Mot de passe** : A5
- **Email** : jmarseille@campus-cci84.fr
- **Nom** : Hyperviseur.itway.local
- **Gateway** : 192.168.150.1
- **DNS** : 8.8.8.8

Stockages

- **Data** : RAID 1 (2x600 Go)
- **Data2** : RAID 5 (4x1,2 To)

9. Machines Virtuelles et Services Communs

Cette section décrit les machines virtuelles (VM) déployées dans l'infrastructure ITWay, leurs services associés, ainsi que les éléments techniques nécessaires à leur fonctionnement et à leur interconnexion. Chaque VM est configurée pour répondre aux besoins communs définis dans le référentiel du BTS SIO SISR, tout en assurant la sécurité, la disponibilité et la performance de l'infrastructure.

9.1 SRVM-ADDS (Active Directory Domain Services)

Objectif principal et rôle du service

- **Objectif** : Centraliser l'authentification et la gestion des identités pour tous les utilisateurs et équipements de l'infrastructure ITWay.
- **Rôle** : SRVM-ADDS héberge un contrôleur de domaine Active Directory (AD-DS) qui permet la gestion des comptes utilisateurs, des groupes de sécurité, des stratégies de groupe (GPO) et des ressources partagées. Il constitue la base de l'authentification pour les services comme GLPI, Radius et les partages de fichiers.

Configuration technique

- **OS** : Windows Server 2022
- **IP** : 10.1.10.3
- **Stockage** : 32 Go
- **Processeur** : 1 (4 cœurs)
- **RAM** : 4096 Mo
- **Utilisateur** : Administrateur
- **Mot de passe** : A5jmkXiP$

Indicateurs de performance et de disponibilité critiques

- **Temps de réponse d'authentification** : < 500 ms pour les requêtes Kerberos/LDAP.
- **Disponibilité** : 99,9 % (redondance prévue avec un second DC à Lille).
- **Taux d'utilisation CPU** : < 70 % en charge normale.
- **Taux de saturation disque** : < 80 % pour éviter les lenteurs dans la gestion des bases NTDS.

Ports et protocoles spécifiques utilisés

- **Port 53 (TCP/UDP)** : DNS pour la résolution des noms de domaine.
- **Port 88 (TCP/UDP)** : Kerberos pour l'authentification sécurisée.
- **Port 135 (TCP)** : RPC pour la réplication AD.
- **Port 389 (TCP/UDP)** : LDAP pour les requêtes d'annuaire.
- **Port 445 (TCP)** : SMB pour les partages de fichiers et SYSVOL.
- **Port 636 (TCP)** : LDAPS pour LDAP sécurisé.
- **Communication inter-services** : SRVM-ADDS fournit l'authentification à SRVM-GLPI (via LDAP), SRVM-FILES (via SMB) et SRVM-Radius (via LDAP/Radius).

9.2 SRVM-MYSQL (Base de données)

Objectif principal et rôle du service

- **Objectif** : Fournir une base de données relationnelle pour stocker et gérer les données des applications utilisées par ITWay.
- **Rôle** : Héberge MariaDB pour les bases de données de GLPI (gestion des incidents) et Radius (authentification Wi-Fi). Ce service est essentiel pour les applications nécessitant un stockage structuré et une haute disponibilité.

Configuration technique

- **OS** : Debian
- **IP** : 10.1.10.7 (interne), 192.168.150.150 (externe)
- **Stockage** : 32 Go
- **Processeur** : 1 (8 cœurs)
- **RAM** : 512 Mo
- **Utilisateur** : root
- **Mot de passe** : NfDx90!36
- **Bases** :
    - glpi_database (Utilisateur : glpi, Mot de passe : RvTch7yHt)
    - radius (Mot de passe : C5Y9h4Vv!)

Indicateurs de performance et de disponibilité critiques

- **Temps de réponse des requêtes SQL** : < 200 ms pour les requêtes simples.
- **Disponibilité** : 99,8 % (sauvegardes régulières via Proxmox).
- **Taux d'utilisation RAM** : < 80 % pour éviter les swaps.

- **Nombre de connexions simultanées** : < 50 pour éviter la saturation.

Ports et protocoles spécifiques utilisés

- **Port 3306 (TCP)** : MySQL/MariaDB pour les connexions clientes.
- **Communication inter-services** :
    - SRVM-GLPI se connecte à SRVM-MYSQL via le port 3306 pour accéder à glpi_database.
    - SRVM-Radius utilise également le port 3306 pour stocker les informations d'authentification Radius.

9.3 SRVM-VPN (Serveur VPN)

Objectif principal et rôle du service

- **Objectif** : Assurer une connexion sécurisée entre les sites de Marseille et Lille.
- **Rôle** : Héberge une instance OpenVPN pour établir un VPN site-à-site, permettant une communication chiffrée entre les deux sites et un accès distant sécurisé pour les administrateurs.

Configuration technique

- **OS** : Debian
- **IP** : 192.168.150.31
- **Stockage** : 32 Go
- **Processeur** : 1 (8 cœurs)
- **RAM** : 8512 Mo
- **Utilisateur** : root
- **Mot de passe** : J4Lh39fy4f7wLD
- **IP VPN** : 192.168.170.1
- **Port externe** : 48009
- **Port interne** : 51820
- **Clés** :
    - Privée : GDD/AkMXVGyB5bHTVHVDjli0yaC1gxuq+HXAm4BRiVQ=
    - Publique : It2JCWhG+3meyw6JdZnSoGzpr/MTMoFzPBXvK3EHnw4=

Indicateurs de performance et de disponibilité critiques

- **Latence VPN** : < 50 ms entre Marseille et Lille.

- **Débit** : > 50 Mbps pour supporter les transferts de fichiers.
- **Disponibilité** : 99,9 % (service critique pour l'interconnexion).
- **Taux d'erreurs de connexion** : < 1 %.

Ports et protocoles spécifiques utilisés

- **Port 48009 (UDP)** : OpenVPN pour le tunnel site-à-site (redirigé depuis l'IP WAN).
- **Port 51820 (UDP)** : WireGuard (option alternative, en test).
- **Communication inter-services** :
    - SRVM-VPN interconnecte SRVM-ADDS et SRVL-ADDS (Lille) pour la réplication AD via le tunnel.
    - Permet l'accès à SRVM-FILES depuis Lille via SMB.

9.4 SRVM-GLPI (Gestion des incidents)

Objectif principal et rôle du service

- **Objectif** : Gérer les incidents et les demandes informatiques au sein d'ITWay.
- **Rôle** : Héberge GLPI, une solution open-source de gestion des tickets et des assets, intégrée à Active Directory pour l'authentification et à MariaDB pour le stockage des données.

Configuration technique

- **IP** : 10.1.10.17
- **Utilisateur** : root ou SRVM-GLPI
- **Mot de passe** : DJ8a69ie9C
- **Utilisateur GLPI** : glpi_user
- **Mot de passe GLPI** : RvTch7yHt
- **Lien** : glpi_g9.itway.local

Indicateurs de performance et de disponibilité critiques

- **Temps de chargement des tickets** : < 2 secondes.
- **Disponibilité** : 99,5 % (redondance en cours de planification).
- **Nombre d'utilisateurs simultanés** : < 30 pour éviter les lenteurs.
- **Taux d'utilisation disque** : < 75 %.

Ports et protocoles spécifiques utilisés

- **Port 80 (TCP)** : HTTP pour l'accès à l'interface web.
- **Port 443 (TCP)** : HTTPS (prévu pour sécurisation future).
- **Port 389 (TCP)** : LDAP pour l'authentification via SRVM-ADDS.
- **Port 3306 (TCP)** : Connexion à SRVM-MYSQL pour la base glpi_database.

9.5 SRVM-FILES (Serveur de fichiers)

Objectif principal et rôle du service

- **Objectif** : Fournir un espace de stockage centralisé et sécurisé pour les données des différents services d'ITWay.
- **Rôle** : Héberge des dossiers partagés accessibles via SMB, gérés par des groupes de sécurité Active Directory et mappés automatiquement via GPO.

Configuration technique

- **IP** : 10.1.1.5
- **Utilisateur** : Administrateur
- **Mot de passe** : xGW64ayt263BxW

Indicateurs de performance et de disponibilité critiques

- **Temps d'accès aux fichiers** : < 100 ms en local, < 200 ms via VPN.
- **Disponibilité** : 99,8 % (sauvegardes régulières).
- **Débit de transfert** : > 100 Mbps.
- **Espace disque utilisé** : < 85 %.

Ports et protocoles spécifiques utilisés

- **Port 445 (TCP)** : SMB pour l'accès aux partages de fichiers.
- **Port 389 (TCP)** : LDAP pour la vérification des autorisations via SRVM-ADDS.
- **Communication inter-services** : Accessible depuis tous les VLANs utilisateurs via VPN ou localement.

9.6 SRVM-Radius (Serveur Radius)

Objectif principal et rôle du service

- **Objectif** : Sécuriser l'accès au réseau Wi-Fi interne via une authentification centralisée.
- **Rôle** : Fournit un serveur Radius pour l'authentification 802.1X des terminaux mobiles et PC connectés au Wi-Fi (VLNM-030).

Configuration technique

- **IP** : 10.1.10.6
- **Utilisateur** : root
- **Mot de passe** : ph5vQUnjo
- **Liens** :
    - Portail utilisateur : http://10.1.10.6
    - Gestion : http://10.1.10.6:8000/

Indicateurs de performance et de disponibilité critiques

- **Temps d'authentification Wi-Fi** : < 1 seconde.
- **Disponibilité** : 99,9 % (critique pour l'accès réseau).
- **Nombre de connexions simultanées** : < 50.
- **Latence réseau** : < 20 ms.

Ports et protocoles spécifiques utilisés

- **Port 1812 (UDP)** : Radius Authentication.
- **Port 1813 (UDP)** : Radius Accounting.
- **Port 3306 (TCP)** : Connexion à SRVM-MYSQL pour la base radius.
- **Port 389 (TCP)** : LDAP pour l'intégration avec SRVM-ADDS.
- **Communication inter-services** : Interagit avec la borne Wi-Fi (10.1.10.7) et SRVM-ADDS.

9.7 SRVM-Nagios (Supervision)

Objectif principal et rôle du service

- **Objectif** : Surveiller la disponibilité et la qualité des équipements et services réseau.
- **Rôle** : Héberge Nagios pour superviser les serveurs, switches, routeurs et services critiques, avec remontée d'alertes en cas d'anomalie.

Configuration technique

- **IP** : 10.1.10.13
- **Utilisateur** : nagios
- **Mot de passe** : nna3xy-pesqez
- **Lien** : 10.1.10.13/nagios

Indicateurs de performance et de disponibilité critiques

- **Temps de réponse des sondes** : < 5 secondes.
- **Disponibilité** : 99,9 % (essentiel pour la supervision).
- **Taux d'utilisation CPU** : < 60 %.
- **Délai d'alerte** : < 1 minute après détection d'une panne.

Ports et protocoles spécifiques utilisés

- **Port 80 (TCP)** : HTTP pour l'interface web.
- **Port 443 (TCP)** : HTTPS (prévu).
- **Port 161 (UDP)** : SNMP pour la supervision des équipements réseau.
- **Communication inter-services** : Supervise SRVM-ADDS, SRVM-MYSQL, SRVM-VPN, etc.

Synthèse des interconnexions

- **SRVM-ADDS** : Fournit l'authentification à SRVM-GLPI, SRVM-FILES, SRVM-Radius via LDAP/Kerberos.
- **SRVM-MYSQL** : Base de données pour SRVM-GLPI et SRVM-Radius.
- **SRVM-VPN** : Relie Marseille et Lille pour l'accès aux services distants.
- **SRVM-Nagios** : Surveille l'ensemble des VMs et équipements physiques.

10. Sauvegarde et Continuité d'Activité

Sauvegarde Proxmox

Pour garantir la continuité des services critiques d'ITWay, une solution de sauvegarde a été implémentée via Proxmox, l'hyperviseur utilisé pour gérer les machines virtuelles (VM) des sites de Marseille et Lille. Voici ce qui a été réalisé :

- **Configuration dans Proxmox** : Une tâche de sauvegarde quotidienne a été planifiée depuis l'interface web de Proxmox pour toutes les VMs critiques (contrôleur de domaine, serveur de fichiers, serveur GLPI, etc.). Le stockage de sauvegarde a été configuré sur un disque dur externe connecté au serveur Proxmox, monté sous /mnt/backup. Le mode "Snapshot" a été choisi pour minimiser les interruptions, avec une compression LZO pour réduire la taille des fichiers.
- **Politique de rétention** : Une stratégie de rétention a été définie : conservation des sauvegardes des 7 derniers jours et d'une sauvegarde hebdomadaire pendant 4 semaines. Cela a permis de disposer de points de restauration multiples en cas de besoin.
- **Tests réalisés** : Une VM GNU/Linux hébergeant un service Samba a été restaurée à partir d'une sauvegarde datée de la veille. Après restauration, les dossiers partagés ont été vérifiés comme accessibles depuis un PC client, validant ainsi la fiabilité du processus.
- **Documentation** : Les étapes de configuration (planification, choix du stockage, tests) ont été consignées dans la documentation technique, avec des captures d'écran de l'interface Proxmox et des commandes exécutées (ex. ls /mnt/backup pour vérifier les fichiers).

Redondances mises en place

Pour assurer la continuité d'activité entre les sites de Marseille et Lille, plusieurs systèmes ont été rendus redondants :

- **AD redondant** : Un deuxième contrôleur de domaine (DC) a été déployé sur une VM Windows Server 2022 à Lille, synchronisé avec le DC principal à Marseille via la réplication AD. La commande repadmin /replsummary a été utilisée pour confirmer que les deux DCs étaient à jour.
- **DHCP redondant** : Deux serveurs DHCP ont été configurés en mode "failover" : un à Marseille (10.0.1.0/24) et un à Lille (10.0.2.0/24). Un relais DHCP a été activé sur le routeur Cisco de Marseille et sur le routeur virtualisé (pfSense) de Lille pour couvrir tous les VLANs.

- **DNS redondant** : Le DNS principal a été hébergé sur le DC de Marseille, avec un serveur secondaire sous BIND sur une VM Ubuntu à Lille. Les zones DNS (ex. itway.local) ont été synchronisées manuellement via des transferts de zone entre les deux serveurs.
- **Pare-feu redondant** : Une instance pfSense a été déployée en cluster CARP (Common Address Redundancy Protocol) entre deux VMs, une par site, pour assurer la continuité des règles de filtrage et du NAT.

Haute Disponibilité et Redondance

Des mécanismes de haute disponibilité (HA) ont été mis en place pour minimiser les interruptions de service :

- **AD, DHCP, DNS** :
    - **Active Directory** : La réplication entre les DCs de Marseille et Lille a été testée en simulant une panne du DC principal (arrêt de la VM). Les clients ont continué à s'authentifier via le DC secondaire, et les GPOs (ex. mappage de lecteurs réseau) sont restées opérationnelles.
    - **DHCP** : En cas d'arrêt d'un serveur DHCP, l'autre a pris le relais sans interruption notable, grâce à la synchronisation des baux vérifiée via les journaux DHCP.
    - **DNS** : Une requête nslookup intranet.itway.local a été exécutée depuis un PC client après arrêt du DNS principal, confirmant que le serveur BIND secondaire répondait correctement.
- **Commutateurs, Routeurs** :
    - **Commutateurs** : Les commutateurs Cisco ont été configurés avec le protocole Spanning Tree (STP) pour éviter les boucles réseau. Une redondance a été testée en débranchant un câble : le trafic a été rerouté via un autre lien sans perte de connectivité.
    - **Routeurs** : À Marseille, le routeur Cisco physique a été couplé à une instance pfSense virtualisée à Lille via VRRP (Virtual Router Redundancy Protocol). Le VPN site-à-site (IPSec) a servi de lien de secours, testé en coupant la connexion principale : le basculement a fonctionné en moins de 10 secondes.

11. Administration et Automatisation

Ansible

Ansible a été déployé pour automatiser la gestion des serveurs ITWay, améliorant l'efficacité administrative :

- **Installation** : Une VM Ubuntu Server a été configurée comme nœud de contrôle Ansible. Le paquet ansible a été installé via apt install ansible, et un fichier d'inventaire (/etc/ansible/hosts) a été créé avec les groupes [serveurs_marseille] (ex. 10.0.1.10) et [serveurs_lille] (ex. 10.0.2.10).
- **Playbooks** : Un playbook a été écrit pour installer et mettre à jour les paquets sur les serveurs Linux (ex. apt: update_cache=yes upgrade=dist). Un autre playbook a configuré Samba sur une VM, en définissant les partages et les permissions via des tâches comme lineinfile pour modifier /etc/samba/smb.conf.
- **Exécution** : Les playbooks ont été testés avec la commande ansible-playbook -i hosts playbook.yml, et leur exécution a été validée par la connexion réussie à un dossier partagé depuis un PC client.

Scripts PowerShell

Des scripts PowerShell ont été développés pour automatiser la gestion d'Active Directory :

- **Script de création d'utilisateur** : Un script a été créé pour ajouter des utilisateurs dans des OU spécifiques (ex. New-ADUser -Name "Jean Dupont" -Path "OU=Commercial,OU=Marseille,DC=itway,DC=local" -AccountPassword (ConvertTo-SecureString "P@ssw0rd" -AsPlainText -Force) -Enabled $true). Ce script a été exécuté sur le DC de Marseille et a permis de peupler l'AD avec les employés fictifs d'ITWay.
- **Script de gestion des GPOs** : Un script a automatisé la création et le lien d'une GPO pour mapper un lecteur réseau (ex. New-GPO -Name "Map_Drive_Commercial" | New-GPLink -Target "OU=Commercial,DC=itway,DC=local"). Le résultat a été vérifié sur un PC client avec gpresult /r.

Déploiement et Gestion des Postes Clients

La gestion des postes clients a été organisée pour répondre aux besoins des utilisateurs d'ITWay :

- **Déploiement** : Les PCs fixes et portables ont été configurés avec Windows 10/11, joints au domaine itway.local via l'AD. Une borne Wi-Fi à Marseille a été mise en place avec une authentification RADIUS (802.1X) liée à l'AD, permettant aux smartphones et tablettes de se connecter sécurellement.
- **Gestion** : Des GPOs ont été appliquées pour installer automatiquement un antivirus (ex. Windows Defender activé via Set-MpPreference -DisableRealtimeMonitoring $false) et configurer le pare-feu Windows. Les dossiers partagés ont été mappés via GPO (ex. \\SRVM-FS\Commercial) pour chaque service.
- **Tests** : Un smartphone a été connecté au Wi-Fi avec les identifiants AD d'un utilisateur commercial, et l'accès au dossier partagé a été validé via une application de gestion de fichiers.

Schéma de câblage détaillé

Un schéma de câblage a été réalisé pour documenter les connexions physiques entre les équipements :

- **Site de Marseille** :
  - **Routeur Cisco** : Interface Gig0/0 connectée à l'IP publique (192.168.150.X) ; Gig0/1 au commutateur principal (port Gig1/0/1, VLAN 10 - Serveurs).
  - **Commutateur principal** : Ports Gig1/0/2 à Gig1/0/5 pour les VMs (VLAN 10), Gig1/0/6 pour la borne Wi-Fi (VLAN 50), Gig1/0/7 vers un second commutateur (trunk avec VTP).
  - **Proxmox** : Connecté au commutateur via une carte réseau sur VLAN 10 (10.0.1.5).
- **Site de Lille** :
  - **Routeur pfSense** : Interface WAN sur 192.168.150.Y, LAN sur VLAN 20 (10.0.2.0/24).
  - **Commutateur virtualisé** : Les VLANs (20 pour serveurs, 30 pour utilisateurs) ont été définis dans Proxmox et propagés via le routeur.
- **Validation** : Le schéma a été dessiné avec un outil comme Visio, incluant les VLANs, IPs, et numéros de ports, puis intégré aux dossiers de situation pour refléter l'infrastructure commune.

Conclusion

Le projet d'infrastructure ITWay, réalisé dans le cadre de l'épreuve E5 du BTS SIO option SISR, a permis de concevoir, déployer et administrer une solution réseau répondant aux besoins d'une entreprise fictive en pleine croissance. En mettant en œuvre une sauvegarde efficace via Proxmox, des redondances critiques (AD, DHCP, DNS, pare-feu) et des mécanismes de haute disponibilité pour les commutateurs et routeurs, nous avons assuré la continuité d'activité entre les sites de Marseille et Lille, tout en respectant les exigences de sécurité et de disponibilité définies par le référentiel. L'automatisation, portée par Ansible et des scripts PowerShell, a optimisé la gestion des serveurs et des postes clients, tandis que le déploiement de ces derniers, accompagné d'un schéma de câblage détaillé, a garanti une infrastructure claire et fonctionnelle.

Ce projet a non seulement permis de maîtriser les technologies imposées (VPN site-à-site, supervision, gestion des configurations), mais aussi de développer des compétences pratiques en résolution de problèmes et en travail collaboratif, essentielles pour un technicien systèmes et réseaux. Les tests réguliers et la documentation rigoureuse ont assuré la fiabilité des solutions mises en place, préparant ainsi efficacement à l'évaluation par le jury. En somme, cette expérience a été une opportunité concrète de traduire les connaissances théoriques en actions techniques opérationnelles, renforçant notre préparation au métier et aux défis de l'informatique professionnelle.