

Matthias RICARD

Lana Pavon

2025/2026



Documentation technique - Projet d'infrastructure

Sommaire

Contexte	2
Présentation	3
Équipe	3
Schéma réseau	3
Schéma Physique	4
Matériel à disposition	4
Conventions:	5
Nommage des VLANs:	5
Nommage des Machines Virtuelles:	5
Paramètres Réseau:	6
Paramètres de comptes:	6
Versions:	7
Cahier des charges + Justifications	7
Services à déployer	7
Haute Disponibilité	7
Routeurs	7
AD	8
Stockage	9
Sauvegardes	9
Supervision	9
Configuration du serveur	10
Disques	10
RAID	10
Stockage	11
Sauvegardes	11
Réseau	11
Marseille	12
Lille	12
Machines Virtuelles	13
Marseille	13
Serveur d'annuaire (SM-WS5-AD)	13
Serveur VPN site à site (SM-DEB-VPN)	14
Serveur de base de données (SM-DEB-SGBD)	14

Gestion des incidents (SM-DEB-GLPI)	14
SIEM / Détection d'intrusions (SM-DEB-WAZUH)	15
Supervision (SM-DEB-CENTREON)	15
Proxy web (SM-ARTI-PROXY)	16
Lille	17
Contrôleur de domaine secondaire (SL-WS5-AD)	17
Routeur principal (RL-OPN-SENSE)	17
Routeur secondaire / Failover (RL-OPN-SENSE2)	18
Client VPN site à site (SL-DEB-VPN)	18
Réplication base de données (SL-DEB-SGBD2)	19
Hors Site	19
VPN d'accès distant (SH-UBU-VPN)	19
Serveur de sauvegardes (SH-PXM-BACKUP)	20
Configurations	20
VPN Site à site	20
Active Directory	20
DNS	20
DHCP	21
Unités d'Organisation (OU)	21
GPO	22
NPS (RADIUS)	22
Politique d'accès réseau	22
Authentification	22
Procédures d'exploitation et de maintenance :	23
Démarrage/arrêt	23
Mises à jour	23
Sauvegardes	23
Supervision	23
Restauration	24
Exploitation des services :	24
Ajout d'un utilisateur :	24
Dossiers partagés :	24
Créer un nouveau VLAN :	24
Sur le Proxmox :	24
Sur les Switch :	25

Intégrer une nouvelle machine :	27
Ajouter un nouvel équipement en supervision :	27
Sécurité	27
Durcissement	28
Segmentation	28
Comptes et droits	28
Politiques de mots de passe	28
Firewall	28
Antivirus	29
Monitoring	29
Sauvegarde hors site	29
Annexes	30
01 - Fichier de configuration OpenVPN de la VM de Marseille.	31
02 - Fichier de configuration OpenVPN de la VM de Lille.	31
03 - Configuration du Routeur de Marseille	32
04 Configuration du switch de Marseille	38
05 Configuration du Switch de Lille	45
06 – Ports switch Marseille	50
07 – Ports switch Lille	51
08-Utilisateurs de la Base de données (SBDG)	51
09- Utilisateurs Active Directory	52
10 - Tableau des services à déployer	52

Contexte

Dans le cadre de l'épreuve E5 du BTS SIO option SISR au sein de la CCI Vacluse, il nous a été demandé de réaliser un projet en groupe portant sur la mise en place d'une infrastructure réseau représentative d'un environnement professionnel. Le projet s'appuie sur l'entreprise fictive ITWay, un fournisseur de services informatiques spécialisé dans l'externalisation de la gestion informatique, le développement de solutions logicielles et la cybersécurité.

ITWay possède deux sites, un à Marseille et un à Lille, que nous avons modélisés dans un environnement virtuel. L'objectif est de connecter ces deux sites grâce à un VPN et de proposer une infrastructure répondant aux besoins d'une entreprise en pleine croissance, tant en matière de performance que de sécurité.

Chaque membre du groupe a participé à la conception et à la mise en œuvre de l'infrastructure commune, avant de développer deux situations professionnelles individuelles autour de problématiques techniques spécifiques.

Ce document présentera la partie commune du projet. Les situations professionnelles seront traitées individuellement dans la suite du dossier.

Présentation

Équipe

Notre groupe est composé de :

- Lana Pavon
- Matthias Ricard

Schéma réseau

Ci-dessous, les schémas réalisés sur draw.io de notre infrastructure :

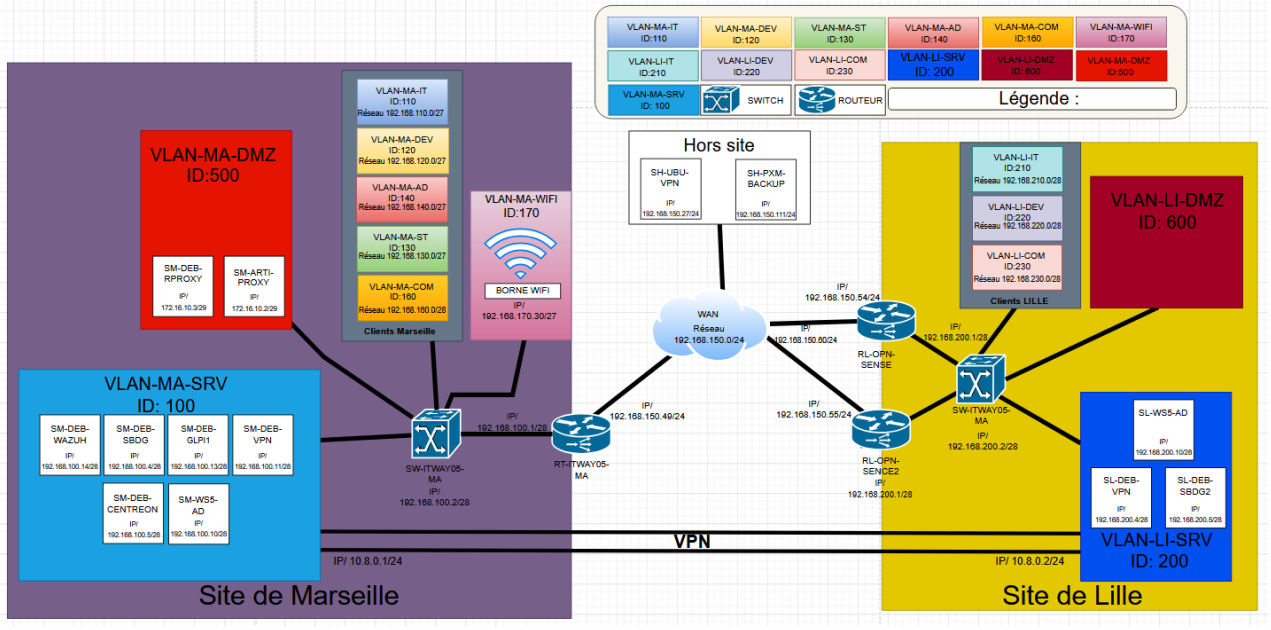
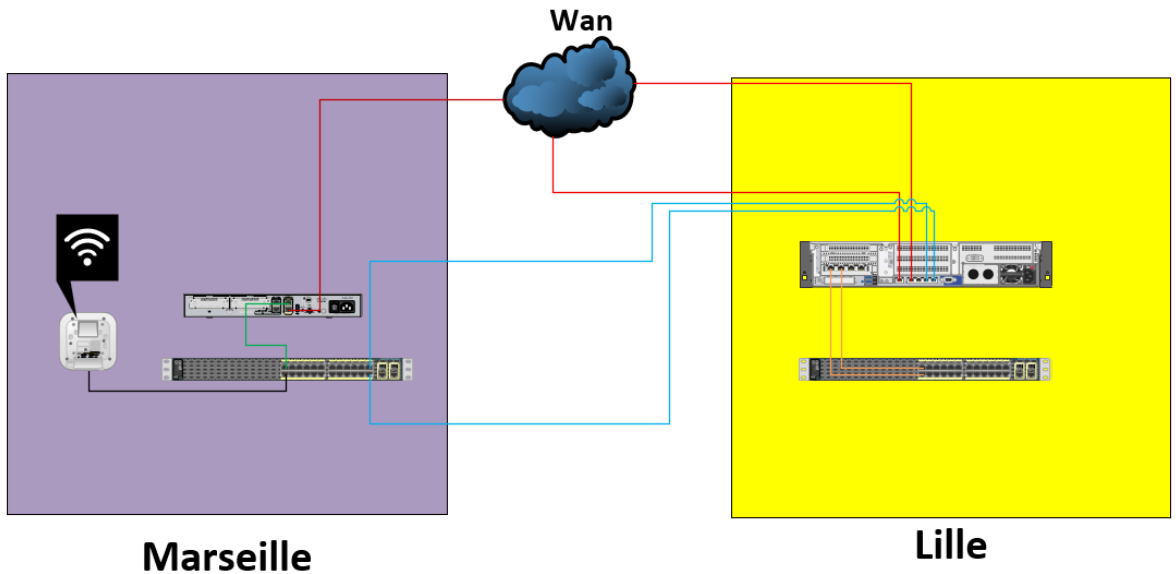


Schéma Physique

Ci-dessous, le schéma physique réalisés sur l’outil Microsoft Visio de notre infrastructure :



Matériel à disposition

Type	Marque	Modèle	“Site”	Ports
Routeur	Cisco	Cisco 1841	Marseille	2

Switch	Cisco	Catalyst 2960-X PoE	Marseille	24
Switch	Cisco	Catalyst 2960	Lille	24
Serveur	HPE	Proliant DL380 Gen10	“Tous”	8
Borne Wifi	ARUBA	AP-105	Marseille	1

Le serveur HPE possède:

- un CPU 40 coeurs
- 62Go de RAM
- 6 disques

Conventions:

Nommage des VLANs:

Nous avons choisi de nommer nos VLAN de cette manière:

VLAN-[Site]-[Service]

Exemple:

VLAN-LI-DEV

Sites:

- LI = Lille
- MA = Marseille

Services:

- SRV = Serveurs
- IT = IT/Management
- DEV = Développement
- ST = Support Technique
- AD = Administratif
- COM = Commercial
- WIFI = Wifi
- DMZ = Zone dématérialisée

Nommage des Machines Virtuelles:

[Type][Site]-[Système d'exploitation]-[Utilisation]

Exemple:

SM-DEB-CENTREON

Types:

- Serveur
- Client
- Routeur

Sites:

- Lille
- Marseille
- Hors site

Systèmes d'exploitations:

- WS5 = Windows Server 2025
- DEB = debian
- UBU = Ubuntu
- PXM = Proxmox
- OPN = OpnSense
- W11 = Windows 11
- W10 = Windows 10

Paramètres Réseau:

Nos routeurs utilisent la première adresse disponible de chaque réseau (192.168.X.1).

Le DHCP est paramétré sur les serveurs Active Directory.

Les machines utilisent respectivement le DNS de l'AD sur leur site (exemple: une machine à Lille utilisera l'AD de Lille comme son DNS).

Le proxy est configuré sur chaque machine de l'infrastructure

Paramètres de comptes:

Chaque machine possède à minima 4 comptes:

- Compte administrateur/root
- Compte "lanap": Compte utilisé par Lana PAVON

- Compte “mricard”: Compte utilisé par Matthias RICARD
- Compte “jury”: Compte pouvant être utilisé par le jury

Versions:

Pour chaque machine/service, la dernière version disponible a été utilisée, sauf en cas d’incompatibilité documentée.

Cahier des charges + Justifications

Services à déployer

Le tableau des services à déployer sur les différents serveurs avec la machine sur laquelle ils ont été déployés est disponible en Annexe n°10.

Haute Disponibilité

Routeurs

Une redondance a été paramétrée sur les routeurs OPNSense de Lille .

Le premier routeur a une ip publique en 192.168.150.54.

Le deuxième a une ip publique en 192.168.150.60.

Ils partagent tous les deux l’IP virtuelle 192.168.150.60.


Les paramètres de synchronisation peuvent être trouvés sur le premier routeur dans “System” > “High Availability” > “Settings”:

System: High Availability: Settings

 advanced mode

General Settings

 Disconnect dialup interfaces

 Synchronize all states via

WAN


 Sync compatibility

OPNsense 24.7 or above

 Synchronize Peer IP

224.0.0.240

Configuration Synchronization Settings (XMLRPC Sync) **Perform synchronization**

 Synchronize Config

192.168.150.55

 Verify peer

 Remote System Username

root

 Remote System Password

••••••••

Services to synchronize (XMLRPC Sync)

 Services

Aliases, Authentication Servers, Captive Portal, Ce

 Clear All

 Select All

Apply

AD

L'AD de Lille est une réplique de celui de Marseille.

C'est-à-dire que si celui de Marseille est éteint ou tombe en panne, celui de Lille prendra le relais, et vice versa.

Ce paramétrage a été fait lors de l'installation de l'AD de Lille qui a rejoint la forêt de l'AD de Marseille :

```

PS C:\WINDOWS\system32> Get-ADForest

ApplicationPartitions : {DC=ForestDnsZones,DC=it-way,DC=local, DC=DomainDnsZones,DC=it-way,DC=local}
CrossForestReferences : {}
DomainNamingMaster    : SVMMA-AD-01.it-way.local
Domains               : {it-way.local}
ForestMode            : Windows2025Forest
GlobalCatalogs       : {SVMMA-AD-01.it-way.local, SL-WS5-AD.it-way.local}
Name                  : it-way.local
PartitionsContainer   : CN=Partitions,CN=Configuration,DC=it-way,DC=local
RootDomain            : it-way.local
SchemaMaster          : SVMMA-AD-01.it-way.local
Sites                 : {Siège-Marseille, Default-First-Site-Name, Antenne-Lille}
SPNSuffixes           : {}
UPNSuffixes           : {}

PS C:\WINDOWS\system32>

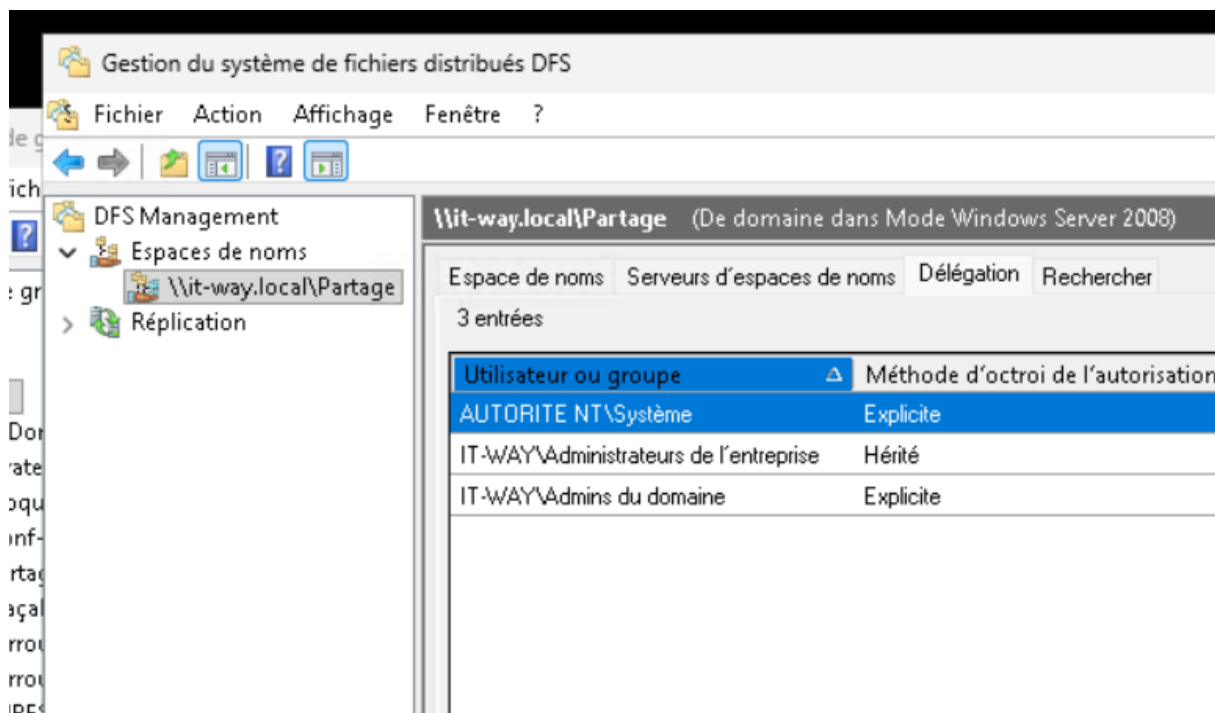
```

Stockage

Pour le stockage des documents, nous avons créé des dossiers partagés redondants.

Les utilisateurs peuvent accéder seulement aux dossiers des services auxquels ils appartiennent (ex: Un utilisateur du service Commercial ne pourra accéder qu'au dossier Commercial).

Ces dossiers partagés redondants ont été paramétrés en utilisant le rôle DFS:



Sauvegardes

Le volume RAID 5 (≈ 3 To) est alloué exclusivement aux VMs de production. Le volume RAID 1 (600 Go) héberge le système Proxmox, les images ISO et la VM de sauvegarde PBS.

Supervision

La VM SM-PXM-BACKUP exécute Proxmox Backup Server sur un disque de 1 To. Les sauvegardes sont déclenchées automatiquement chaque vendredi à 22h00 et conservent au maximum 3 versions. Pour effectuer une sauvegarde manuelle, accéder à l'interface Proxmox → sélectionner la VM → "Backup" → "Backup now".

Configuration du serveur

Disques

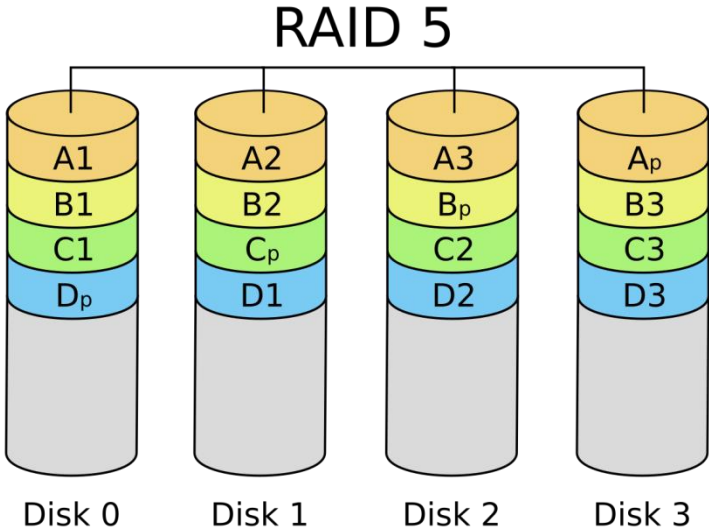
Notre Serveur HPE possède 6 Disques Durs dont 4 de 1.2TB chacun et 2 de 600GB chacun.

RAID

Nous avons "groupé" les disques en 2 groupes:

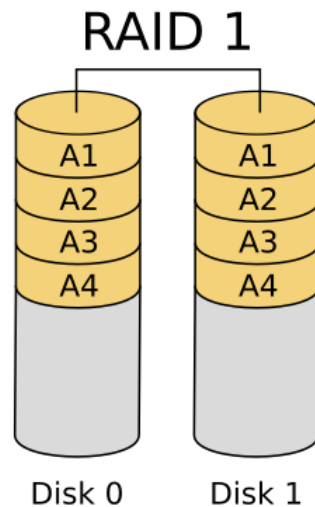
- Les 4 disques de 1.2TB
- Les 2 disques de 600GB

Nous avons utilisé le premier groupe pour créer un "RAID 5". Ce RAID permet une redondance des données sur un seul volume de 3To ici.. Il segmente les données sur les disques de façon à pouvoir les remettre en place si un disque tombe en panne. Le dessin ci-dessous permet une meilleure visualisation:



Le deuxième groupe a été utilisé pour créer un "RAID 1". Ce type de RAID permet une redondance des données en recopiant les données sur les 2 disques à la fois de sorte que si l'un des deux tombe, l'autre prenne le relais en attendant d'être remplacé. Les 2 disques de 600Go forment donc un disque de 600Go (les données sont les mêmes sur

les 2 disques, ils ne sont pas combinés). Le dessin ci-dessous permet une visualisation des disques:



Stockage

Le volume créé avec un RAID 5 plus tôt servira à stocker les machines virtuelles. Celui créé avec le RAID 1 servira à stocker le système, les sauvegardes et les images ISO.

Sauvegardes

Nous avons créé une VM "SM-PXM-BACKUP" avec un disque de 500Go sur laquelle nous avons installé Proxmox Backup Server, un système d'exploitation de proxmox permettant la sauvegarde décentralisée tout en gardant le même écosystème.

Nos sauvegardes ont été paramétrées s'exécuter tous les vendredis à 22:00 et garder maximum 3 sauvegardes.

Réseau

Nous avons utilisé le protocole LACP pour permettre à notre Serveur d'avoir de la redondance au niveau de ses ports. Les ports 3 et 4 du serveur servent à créer un "Bond" pour le trafic des VLANs de Lille et les ports 5 et 6 du serveur sont utilisés pour les VLANs de Marseille.

Pour les switches, les ports 23 et 24 du switch de Marseille sont utilisés pour le "bond" et les ports 1 et 2 du serveur de Lille sont utilisés pour le "bond".

Interfaces du serveur HPE:

Interface	Type	VLAN?	Ports
vmbr0	Linux Bridge	X	nic0
vmbrLi	Linux Bridge	V	bond0
vmbrMa	Linux Bridge	V	bond1
bond0	Linux Bond	X	nic4 nic5
bond1	Linux Bond	x	nic2 nic3

Marseille

Notre réseau de Marseille utilise ses VID comme 3^e octet dans son adresse IP. Le VID 150 n'a pas été utilisé car il correspond au "Internet simulé" de la classe.

Nom	VID	Adresse Réseau	Service	Passerelle	DHCP
VLAN-MA-SRV	100	192.168.100.0/28	Serveurs	.100.1	Aucun
VLAN-MA-IT	110	192.168.110.0/27	IT/Management	.110.1	.110.1 à .110.29
VLAN-MA-DEV	120	192.168.120.0/27	Développement	.120.1	.120.1 à .120.29
VLAN-MA-ST	130	192.168.130.0/27	Support Technique	.130.1	.130.1 à .130.29
VLAN-MA-AD	140	192.168.140.0/27	Administratif	.140.1	.140.1 à .140.29
VLAN-MA-COM	160	192.168.160.0/28	Commercial	.160.1	.160.1 à .160.13
VLAN-MA-WIFI	170	192.168.170.0/27	Wifi	.170.1	.170.1 à .170.29
VLAN-MA-DMZ	500	172.16.10.0/29	Zone dématérialisée	.10.1	Aucun

Lille

Nom	VID	Adresse Réseau	Service	Passerelle	DHCP
VLAN-LI-SRV	200	192.168.200.0/28	Serveurs	.200.1	Aucun
VLAN-LI-IT	210	192.168.210.0/28	IT/Management	.210.1	.210.1 à .210.13
VLAN-LI-DEV	220	192.168.220.0/28	Développement	.220.1	.220.1 à .220.13
VLAN-LI-COM	230	192.168.230.0/28	Commercial	.230.1	.230.1 à .230.13
VLAN-LI-DMZ	600	172.16.20.0/29	Zone dématérialisée	20.1	Aucun

Les configurations des routeurs et switches sont disponibles en Annexe n°[03](#), [04](#) et [05](#).

Machines Virtuelles

Marseille

Les machines virtuelles créées sur le site de Marseille sont détaillées dans le tableau qui suit. Les informations comme l'OS, le type (serveur/client) peuvent être retrouvées dans les noms des machines conformément à la convention de [nommage des machines](#).

La colonne "Ressources" est à lire de cette manière:

- Le premier nombre correspond à la RAM allouée en Go.
- Le 2è nombre correspond au nombre de cœurs de CPU alloués.
- Le 3è nombre correspond au stockage alloué en Go.

VID	Nom	Services installés	Description	Ressources
104	SM-WS5-AD	- ACTIVE DIRECTORY - DNS - DHCP	Serveur de gestion de comptes, de DHCP et DNS	4/2/50
107	SM-DEB-VPN	- OPENVPN	Connexion au site distant (Lille)	2/1/20
110	SM-DEB-SGBD	- MARIADB	Base de données	4/3/50
118	SM-DEB-GLPI	- GLPI	Gestion des incidents	2/2/32
111	SM-DEB-WAZUH	- WAZUH	Détection d'intrusions	4/4/70
116	SM-DEB-CENTREON	- CENTREON	Supervision	2/2/40
121	SM-ARTI-PROXY	- PROXY (artica)	Proxy	4/2/64
113	CM-W11-IT	- Wireshark	Client	4/2/64

Serveur d'annuaire (SM-WS5-AD)

Paramètre	Détails Techniques
OS	Windows Server 2025
Services	AD-DS, DNS, DHCP
IP / VLAN	192.168.100.10 (VLAN 100 — Marseille)
Ressources	4 Go RAM / 2 cœurs / 50 Go disque
Sécurité	Windows Defender, Pare-feu Windows, supervision Centreon et Wazuh

Ce serveur constitue le socle d'authentification et de gestion des ressources du site de Marseille. Le rôle AD-DS gère l'ensemble des objets (utilisateurs, ordinateurs, groupes) du domaine it-way.local. Le DNS résout les noms internes et les entrées spécifiques (aide.it-way.local → 192.168.100.13, supervision.it-way.local → 192.168.100.5). Le DHCP distribue

automatiquement les adresses IP selon les plages définies par VLAN. Une réservation est effectuée dans le VLAN-MA-SRV pour chaque équipement fixe via son adresse MAC.

Serveur VPN site à site (SM-DEB-VPN)

Paramètre	Détails Techniques
OS	Debian 12
Service	OpenVPN (serveur)
IP / VLAN	192.168.100.11 (VLAN 100 — Marseille)
IP tunnel	10.8.0.1/24
Ressources	2 Go RAM / 1 cœur / 20 Go disque
Sécurité	root désactivé en SSH, Fail2Ban, UFW, supervision Centreon et Wazuh

Ce serveur assure le tunnel chiffré permanent entre le site de Marseille et le site de Lille. Il utilise l'outil OpenVPN sur le port UDP 58803. Le chiffrement AES-256-GCM garantit la confidentialité des échanges inter-sites. Les fichiers de configuration complets sont disponibles en Annexe 01 (configuration du serveur Marseille) et Annexe 02 (configuration du client Lille).

Serveur de base de données (SM-DEB-SGBD)

Paramètre	Détails Techniques
OS	Debian 12
Service	MariaDB
IP / VLAN	192.168.100.4 (VLAN 100 — Marseille)
Ressources	4 Go RAM / 3 cœurs / 50 Go disque
Sécurité	root désactivé en SSH, Fail2Ban, UFW, supervision Centreon et Wazuh

Ce serveur centralise toutes les bases de données de l'infrastructure. Il héberge les bases de GLPI et Centreon. L'accès est restreint aux serveurs applicatifs autorisés via des règles UFW. La réplication vers le site de Lille (SL-DEB-SGBD2) assure la continuité de service en cas de panne.

Gestion des incidents (SM-DEB-GLPI)

Paramètre	Détails Techniques
OS	Debian 12
Service	GLPI

IP / VLAN	192.168.100.13 (VLAN 100 — Marseille)
Ressources	2 Go RAM / 2 cœurs / 32 Go disque
Sécurité	root désactivé en SSH, Fail2Ban, UFW, supervision Centreon

GLPI (Gestionnaire Libre de Parc Informatique) permet l'inventaire automatisé du matériel et du logiciel, ainsi que la gestion des demandes d'assistance (ticketing). L'authentification est centralisée sur l'Active Directory. Les agents GLPI sont déployés sur les postes clients via la GPO "GPO-Agent-GLPI". La base de données est hébergée sur SM-DEB-SGBD. L'accès web est sécurisé via HTTPS.

SIEM / Détection d'intrusions (SM-DEB-WAZUH)

Paramètre	Détails Techniques
OS	Debian 12
Service	Wazuh (Manager + Dashboard)
IP / VLAN	192.168.100.14 (VLAN 100 — Marseille)
Ressources	4 Go RAM / 4 cœurs / 70 Go disque
Sécurité	root désactivé en SSH, Fail2Ban, UFW, supervision Centreon

Wazuh est la solution SIEM (Security Information and Event Management) de l'infrastructure. Elle collecte et analyse en temps réel les logs et événements de sécurité de tous les équipements. Les agents Wazuh sont déployés sur chaque serveur via la GPO "GPO-Agent-Wazuh". Le tableau de bord permet de visualiser les alertes de sécurité, les tentatives de connexion échouées, les modifications de fichiers système et les anomalies réseau. Des règles personnalisées permettent d'alerter l'équipe IT en cas d'incident.

Supervision (SM-DEB-CENTREON)

Paramètre	Détails Techniques
OS	Debian 12
Service	Centreon
IP / VLAN	192.168.100.5 (VLAN 100 — Marseille)
Ressources	2 Go RAM / 2 cœurs / 40 Go disque
Sécurité	root désactivé en SSH, Fail2Ban, UFW

Centreon assure la supervision centralisée de l'ensemble de l'infrastructure ITWay (deux sites). Il surveille la disponibilité des services, l'état de santé du matériel et les performances réseau. Les métriques sont collectées via SNMP v2c pour les équipements Cisco, et via des agents sur les serveurs Linux/Windows.

L'interface est accessible à l'URL <https://supervision.it-way.local>.

Liste des machines supervisées :

Nom	IP	Services supervisés
SM-DEB-SGBD	192.168.100.4	<ul style="list-style-type: none"> - CPU - Load - Memory - Ping - Swap
SL-DEB-POLLER	192.168.200.12	<ul style="list-style-type: none"> - Ping
SM-DEB-VPN	192.168.100.11	<ul style="list-style-type: none"> - CPU - Load - Memory - Ping - Swap
SM-DEB-WAZUH	192.168.100.14	<ul style="list-style-type: none"> - CPU - Load - Memory - Ping - Swap
SM-WS5-AD	192.168.100.10	<ul style="list-style-type: none"> - CPU - Memory - Ping - Swap

Proxy web (SM-ARTI-PROXY)

Paramètre	Détails Techniques
OS	Debian 12
Service	Artica Proxy
IP / VLAN	172.16.10.2 (VLAN 500 — DMZ Marseille)
Ressources	4 Go RAM / 2 cœurs / 64 Go disque
Sécurité	root désactivé en SSH, Fail2Ban, UFW, supervision Centreon

Le proxy Artica est le point de passage unique entre le réseau interne et Internet pour le site de Marseille. Il filtre la navigation des collaborateurs, bloque les domaines malveillants ou non productifs, et met en cache les ressources fréquentes. La configuration proxy est poussée automatiquement sur tous les postes via la GPO "GPO-Conf-PROXY".

Lille

De la même manière que pour la liste de machines de Marseille, certaines informations peuvent être trouvées dans le nom des machines conformément à la

[Convention de nommage des machines](#)

VID	Nom	Services Installés	Description	Ressources
108	SL-WS5-AD	- Active Directory - DHCP - DNS	Serveur de gestion de comptes, de DHCP et DNS	4/2/50
120	RL-OPN-SENSE	- SNMP	Routeur principal de Lille	4/2/75
101	RL-OPN-SENSE2	- SNMP	Routeur Secondaire	4/2/75
109	SL-DEB-SGBD2	- Mariadb	Serveur de redondance de la base de données	2/1/50
119	SL-DEB-VPN	- OpenVPN	Serveur du VPN site à site	2/1/20

Contrôleur de domaine secondaire (SL-WS5-AD)

Paramètre	Détails Techniques
OS	Windows Server 2025
Services	AD-DS, DNS, DHCP
IP / VLAN	192.168.200.10 (VLAN 200 — Lille)
Ressources	4 Go RAM / 2 cœurs / 50 Go disque
Sécurité	Windows Defender, Pare-feu Windows, supervision Centreon

Ce serveur est intégré à la forêt it-way.local, il héberge un contrôleur de domaine secondaire qui réplique les objets AD depuis Marseille via le tunnel VPN. En cas de rupture du lien inter-sites, les utilisateurs de Lille peuvent continuer à s'authentifier localement. Le rôle DFS-R assure la réplication du partage de fichiers et du dossier SYSVOL entre les deux sites.

Routeur principal (RL-OPN-SENSE)

Paramètre	Détails Techniques
OS	OPNsense (basé FreeBSD)
Services	Routage inter-VLAN, Firewall, VPN OpenVPN
IP LAN	192.168.200.1 (VLAN 200 — Lille)
IP WAN	192.168.150.54

Ressources	4 Go RAM / 2 cœurs / 75 Go disque
------------	-----------------------------------

OPNsense est le routeur du site de Lille. Il assure le routage entre tous les VLANs locaux (SRV, IT, DEV, COM, DMZ), filtre les flux entrants et sortants via des règles firewall, et maintient le tunnel VPN permanent avec le site de Marseille. Les règles de firewall interdisent les flux non essentiels entre VLANs. Seuls les flux d'administration (AD, DNS, Centreon) et les services autorisés sont permis. La configuration est synchronisée avec le routeur secondaire via XMLRPC.

Routeur secondaire / Failover (RL-OPN-SENSE2)

Paramètre	Détails Techniques
OS	OPNsense (basé FreeBSD)
Services	Routage inter-VLAN, Firewall, VPN (failover)
IP LAN	192.168.200.1 (VLAN 200 — Lille)
IP WAN	192.168.150.60
Ressources	4 Go RAM / 2 cœurs / 75 Go disque

Ce routeur fonctionne en mode passif (failover). Les deux routeurs partagent une adresse IP virtuelle (VIP CARP) qui sert de passerelle par défaut pour tous les clients. Si le routeur principal tombe, l'esclave prend automatiquement le relais en quelques secondes, sans intervention humaine. Toutes les règles firewall, configurations DHCP et paramètres VPN sont répliqués depuis le principal via XMLRPC. Ce serveur garantit la continuité du service réseau et du tunnel inter-sites même en cas de panne matérielle.

Client VPN site à site (SL-DEB-VPN)

Paramètre	Détails Techniques
OS	Debian 12
Service	OpenVPN (client)
IP / VLAN	192.168.200.4 (VLAN 200 — Lille)
IP tunnel	10.8.0.2/24
Ressources	2 Go RAM / 1 cœur / 20 Go disque
Sécurité	root désactivé en SSH, Fail2Ban, UFW

Ce serveur établit la connexion permanente vers le serveur VPN de Marseille (SM-DEB-VPN, 10.8.0.1). Le tunnel chiffré AES-256-GCM permet aux deux sites d'échanger des données comme s'ils étaient sur le même réseau local. Tous les flux destinés aux réseaux de

Marseille (192.168.100.0/28) sont routés dans ce tunnel. Le fichier de configuration complet est disponible en Annexe 02.

Réplication base de données (SL-DEB-SGBD2)

Paramètre	Détails Techniques
OS	Debian 12
Service	MariaDB (mode Slave — lecture seule)
IP / VLAN	192.168.200.5 (VLAN 200 — Lille)
Ressources	2 Go RAM / 1 cœur / 50 Go disque
Sécurité	root désactivé en SSH, Fail2Ban, UFW, supervision Centreon

Ce serveur maintient une copie synchronisée en temps réel des bases de données hébergées sur SM-DEB-SGBD à Marseille. Il fonctionne en mode "Slave" de réplication MariaDB : le maître enregistre chaque modification dans ses Binary Logs, l'esclave se connecte et rejoue ces logs localement. En fonctionnement normal, l'esclave est en lecture seule. En cas de défaillance du maître, il peut être promu manuellement pour assurer la continuité des services qui dépendent de la base de données.

Hors Site

VID	Nom	Services installés	Description	Ressources
100	SH-UBU-VPN	- OpenVPN	VPN permettant l'accès à l'infrastructure	4/2/20
122	SH-PXM-BACKUP	- Proxmox Backup	Serveur de Sauvegardes	4/3/40

VPN d'accès distant (SH-UBU-VPN)

Paramètre	Détails Techniques
OS	Ubuntu 24.04 LTS
Service	OpenVPN
IP	192.168.150.27 (hors site)
Ressources	4 Go RAM / 2 cœurs / 20 Go disque
Sécurité	root désactivé en SSH, Fail2Ban, UFW, supervision Centreon

Ce serveur permet aux collaborateurs nomades d'ITWay d'accéder aux ressources internes depuis n'importe quelle connexion Internet. Le chiffrement AES-256-GCM protège toutes les données échangées. Une fois connecté, l'utilisateur accède aux ressources de Marseille et de Lille comme s'il était sur site.

Serveur de sauvegardes (SH-PXM-BACKUP)

Paramètre	Détails Techniques
OS	Proxmox Backup Server (PBS)
IP	192.168.150.111 (hors site)
Ressources	4 Go RAM / 3 cœurs / 500 Go disque

PBS est la solution de sauvegarde externalisée de l'infrastructure. Il utilise la déduplication et la compression pour minimiser l'espace de stockage et la bande passante. Les données sont chiffrées par Proxmox avant envoi.

Configurations

VPN Site à site

Le VPN site à site est configuré avec 2 VMs pouvant être retrouvées dans la [liste des VMs](#).

Les fichiers de configuration OpenVPN de chaque VM sont disponibles en Annexe [01](#) et [02](#).

Le serveur SM-DEB-VPN a dans ce réseau l'IP 10.8.0.1/24.

Le serveur SL-DEB-VPN a dans ce réseau l'IP 10.8.0.2/24.

Active Directory

Le service Active Directory permet aux utilisateurs de s'authentifier.

Les utilisateurs peuvent joindre ce domaine avec le nom "it-way.local" et leur nom d'utilisateur.

DNS

Les serveurs AD ont le rôle DNS installé, permettant de résoudre les domaines suivants vers les IP locales suivantes :

Entrée DNS	IP visée
aide.it-way.local	192.168.100.13

supervision.it-way.local	192.168.100.5
--------------------------	---------------

DHCP

Les serveurs AD ont aussi le rôle DHCP installé. Il distribue les IPs en fonction de la plage DHCP du tableau des VLANs, dans la [colonne DHCP](#).

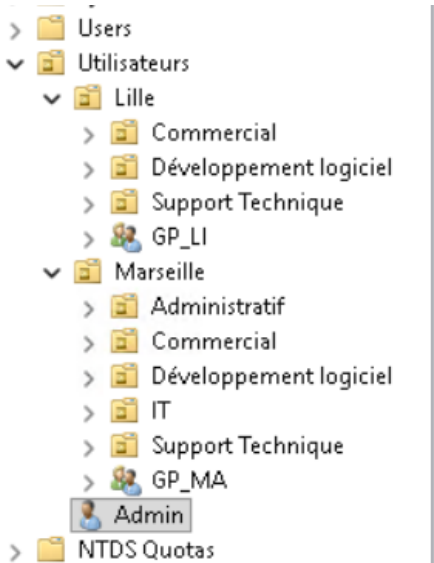
Unités d’Organisation (OU)

Voici un tableau récapitulatif de l'arborescence des OU :

Utilisateurs

- Lille**
- Développement logiciel
 - Support Technique
 - Administratif
 - Commercial

- Marseille**
- Développement logiciel
 - IT
 - Support Technique



GPO

Nom	Usage	Objectif
GPO-Agent-GLPI	Elle permet d'avoir l'agent GLPI d'installer sur tous les postes du domaine	Supervision
GPO-Agent-Wazuh	Elle permet d'avoir l'agent WAZUH d'installer sur tous les postes du domaine	Securité
GPO-Partage	Elle permet d'ajouter la configuration du Lecteur réseau pour le partage réseau	Automatisation
GPO-WIRESHARK	Elle permet d'avoir Wireshark d'installer sur tous les postes du domaine	Outil d'analyse réseau

NPS (RADIUS)

L'implémentation du service **RADIUS** (*Remote Authentication Dial-In User Service*) constitue une brique de sécurité critique visant à centraliser et à renforcer le contrôle des accès aux ressources réseau de l'organisation.

Politique d'accès réseau

Seuls les employés qui ont un compte dans l'active Directory ont la possibilité de se connecter au Wifi.

Authentification

Tous les utilisateurs se connecteront en utilisant leurs identifiants et mots de passes Active Directory (format p.nom) sur le point d'accès ayant pour nom "ITWAY-G5".

Procédures d'exploitation et de maintenance :

Démarrage/arrêt

Pour éteindre le serveur Proxmox, il faut d'abord éteindre chaque VM manuellement et ensuite éteindre le serveur.

Pour démarrer le serveur, il suffit d'allumer le serveur, les VMs nécessaires sont paramétrées pour démarrer automatiquement.

Mises à jour

Toutes les machines ont des “tâches cron” leur permettant de mettre leurs dépôts à jour. Si d’autres services ont besoin de mises à jour, ils sont aussi paramétrés dans les tâches cron de chaque machine.

Sauvegardes

La machine “SRV-PXM-BACKUP” permet d’automatiser les sauvegardes tout en gardant un environnement Proxmox. Les sauvegardes sont paramétrées pour être exécutées tous les vendredis à 22 heure.

Les sauvegardes peuvent être trouvées dans “pve-backup > Backup”.

Pour effectuer une sauvegarde manuelle, aller sur la machine puis dans backup et cliquer sur backup pour faire un backup.

Supervision

Les machines sont supervisées sur l’interface graphique de Centreon (<https://supervision.it-way.local>).

Pour rajouter un appareil dans la supervision il faut installer snmp sur la machine à superviser:

```
apt install snmpd
```

Et modifier le fichier “/etc/snmp/snmpd.conf” pour s’assurer d’avoir ces paramètres:

```
view centreon included .1.3.6.1 rocommunity centreonSNMP 192.168.100.5 -V centreon  
rocommunity centreonSNMP 192.168.100.5
```

Ensuite sur l’interface de centreon (supervision.it-way.local) et rentrer les informations de la machine:

[Host Configuration](#)
[Notification](#)
[Relations](#)
[Data Processing](#)
[Host Extended Infos](#)

| Add a Host

Host basic information

Name *

Alias

Address * Resolve

SNMP Community & Version ▼

Monitoring server Central ▼

Timezone Timezone ▼ ⓘ

Templates
 A host or host template can have several templates. See help for more details.

[+ Add a new entry](#)
 Nothing here, use the "Add" button

Create Services linked to the Template too Yes No

Host check options

Check Command Check Command ▼ ⓘ ⊗

Args ←

Custom macros
■ Template inheritance

[+ Add a new entry](#)
 Nothing here, use the "Add" button

Restauration

Pour restaurer une sauvegarde il suffit de cliquer dessus puis sur “Restore”/”Restaurer”.

Exploitation des services :

Ajout d’un utilisateur :

Dans le logiciel “Utiisateurs de l’active directory”, faire un clic droit sur l’équipe dans laquelle l’utilisateur doit être et cliquer sur “Nouvel utilisateur” puis rentrer les informations nécessaires.

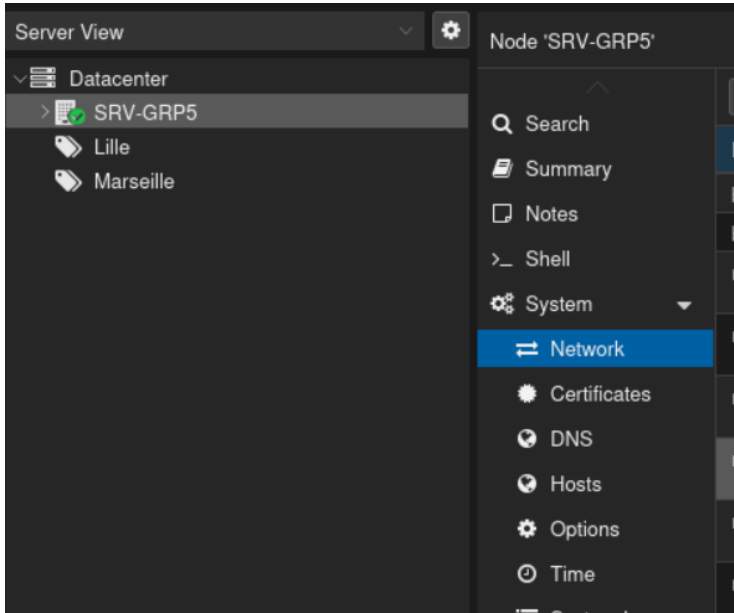
Dossiers partagés :

Les dossiers partagés sont paramétrés via les paramètres de chaque compte utilisateur.

Créer un nouveau VLAN :

Sur le Proxmox :

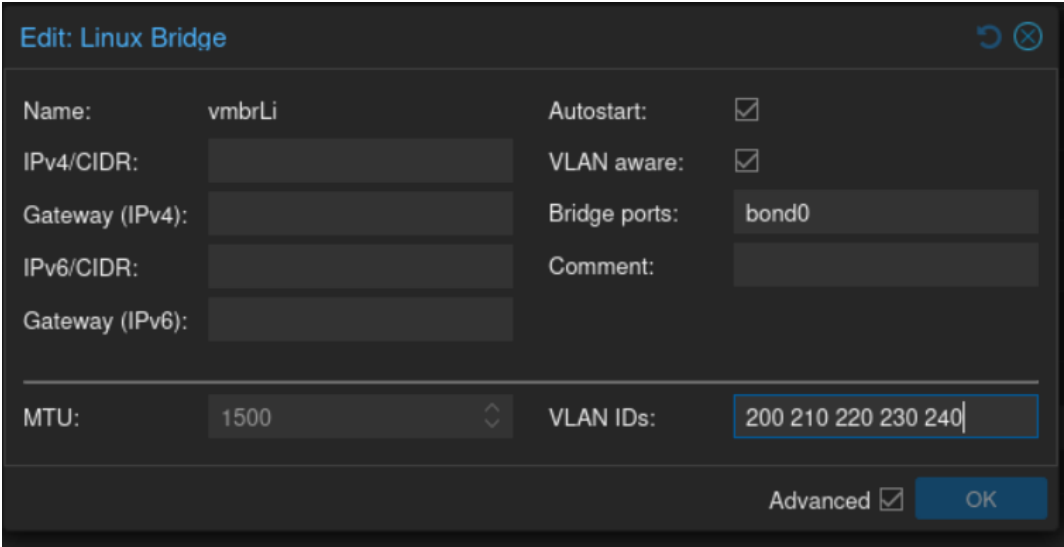
Se connecter à l’interface Proxmox puis aller dans SRV-GRP5 > Network



Puis choisir le site souhaité et modifier :

vibrLi	Linux Bridge	Yes	Yes	Yes	bond0
vibrMa	Linux Bridge	Yes	Yes	Yes	bond1

Et rajouter ou enlever le VLAN souhaité :

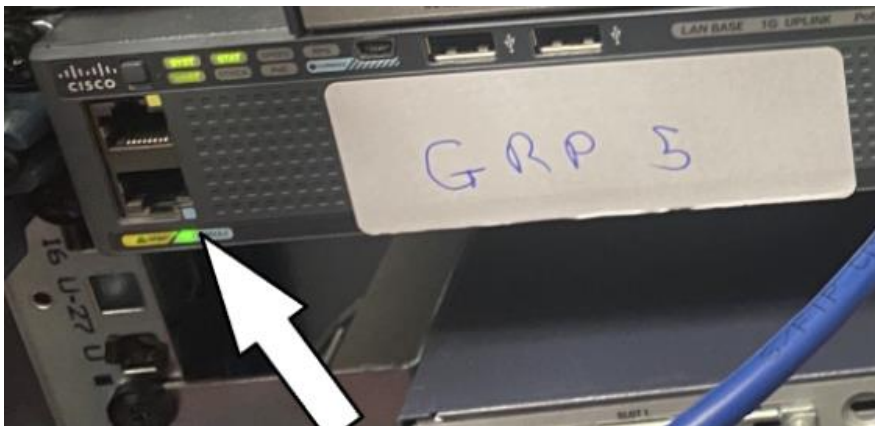


Sur les Switch et le routeur (MA):

Se connecter soit en serial via un câble rs232 sur le switch



Via le port console du switch :



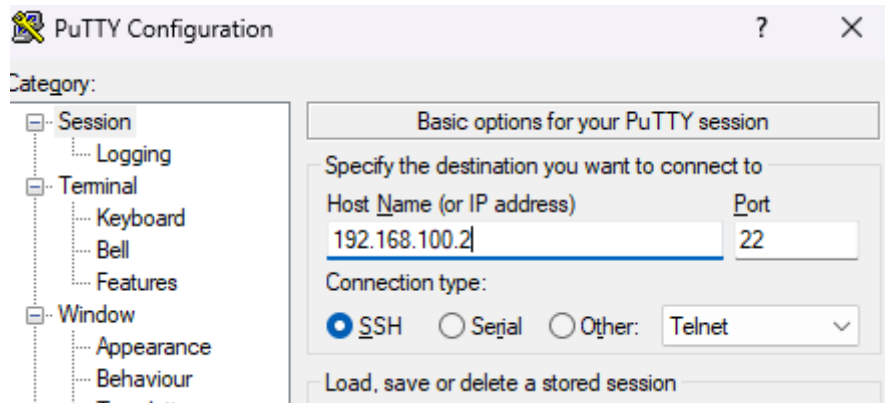
Utiliser l'outil PuTTY

Pour le mettre en mode "série", il vous suffit de cliquer sur "Serial". Entrez ensuite le port utilisé pour connecter votre machine au switch, et, si ce n'est pas déjà le cas, entrez la valeur "9600" pour la vitesse en bits/seconde.

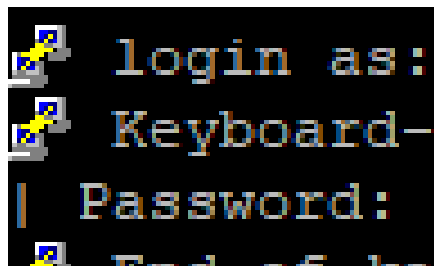
Specify the destination you want to connect to	
Serial line	Speed
COM1	9600
Connection type:	
<input type="radio"/> SSH	<input checked="" type="radio"/> Serial
<input type="radio"/> Other:	Telnet

Ou se connecter en SSH au switch ((Marseille :192.168.100.2) ou (L'ille : 192.168.200.2)) ou au routeur Marseille (192.168.100.1)

Grace a l'outil PuTTY



Ensuite se connecter avec les identifiants de la machine :



Ensuite taper les commandes suivantes :

```
en
conf terminal
vlan (numéro du vlan)
name (nom du vlan)
```

Pour vérifier que le vlan est bien créé vous pouvez faire la commande suivante :

```
do show vlan
```

Intégrer une nouvelle machine :

Se rendre dans les paramètres de l'ordinateur et aller dans "Compte" > *Accès professionnel ou scolaire" > Se connecter > Se connecter avec un compte Active Directory. Se connecter avec le nom de domaine it-way.local et les informations d'identification.

Ajouter un nouvel équipement en supervision :

Dans l'interface Web de Centreon, aller dans "Configuration" > "Hôtes" puis cliquer sur "Ajouter" et remplir les informations nécessaires.

Sécurité

Durcissement

Nom	Type	IP source	IP dest.	Protocole	Port
ACL_FROM_DMZ	Permit	Any	172.16.10.0/29	TCP	established
	Permit	Any	172.16.10.0/29	TCP	www(80) (HTTP)
	Permit	Any	172.16.10.0/29	TCP	443 (HTTPS)
	Permit	Any	172.16.10.0/29	TCP	3128 (Proxy)
	Permit	172.16.10.0/29	Any	IP (Tous)	Tous
	Denny	Any	Any	IP (Tous)	Tous

Segmentation

Pour la segmentation de l'infrastructure nous avons fait le choix de segmenter notre réseau en plusieurs vlan.

Comptes et droits

Les 4 comptes présents sur toutes les machines (root, lanap, mricard et jury) ont tous des droits administrateurs, les autres comptes sont juste des utilisateurs simples.

Politiques de mots de passe

Caractéristiques :

- Minimum 8 **caractères**
- Majuscules (A-Z)
- Minuscules (a-z)
- Chiffres (0-9)
- Caractères spéciaux (!@#\$%^&* _-+=)

Interdictions :

- Pas de prénoms, noms, dates de naissance
- Pas de réutilisation d'un ancien mot de passe
- Pas de séquences évidentes

Firewall

Nous avons retenu OPNsense comme firewall car il offre une protection réseau complète et fiable tout en restant flexible grâce à son modèle open source.

Antivirus

Nous avons choisi Windows Defender car il offre une protection complète, intégrée et constamment mise à jour pour notre environnement Windows. Sa gestion centralisée, ses capacités avancées de détection et son intégration native avec nos outils Microsoft renforcent la sécurité tout en simplifiant l'administration. C'est une solution efficace, fiable et économique pour protéger notre infrastructure.

Monitoring

Nous avons choisi Centreon pour superviser notre infrastructure car il s'agit d'une solution fiable, complète et parfaitement adaptée à la diversité de notre environnement. Grâce à ses nombreux connecteurs prêts à l'emploi, Centreon permet un déploiement rapide et une supervision standardisée de nos serveurs, équipements réseau et services cloud, sans développements spécifiques.

La plateforme offre une visibilité claire sur l'état du système d'information grâce à des tableaux de bord personnalisables et une approche orientée services, ce qui facilite l'identification des incidents et l'évaluation de leur impact sur les activités métiers. Sa gestion efficace des alertes améliore notre réactivité et réduit les interruptions de service.

Enfin, Centreon s'intègre facilement avec nos outils existants et répond aux exigences actuelles en matière de sécurité, ce qui en fait une solution pérenne et évolutive pour accompagner la croissance de notre infrastructure.

Sauvegarde hors site

La sauvegarde hors site est effectuée via le Serveur Proxmox Backup Server (SH-PXM-BACKUP). La VM étant paramétrée dans le réseau de l'école (Internet simulé), elle fait office de VM hors-site. La sauvegarde est donc hors site.

Annexes

01 - Fichier de configuration OpenVPN de la VM de Marseille.

```
ort 58803
proto udp
dev tun
ca ca.crt
cert server.crt
key server.key
dh dh.pem
auth SHA256
tls-auth ta.key 0
topology subnet
server 10.8.0.0 255.255.255.0 # Réseau virtuel du VPN
ifconfig-pool-persist ipp.txt
push "redirect-gateway def1 bypass-dhcp" # Pour faire passer tout le trafic par le VPN
push "dhcp-option DNS 8.8.8.8"
keepalive 10 120
cipher AES-256-GCM
user nobody
group nogroup
persist-key
persist-tun
status openvpn-status.log
verb 3
route 192.168.200.0 255.255.255.240
push "route 192.168.100.0 255.255.255.240"
client-config-dir /etc/openvpn/ccd
```

02 - Fichier de configuration OpenVPN de la VM de Lille.

```
client
dev tun
proto udp
remote 192.168.150.49 58803
resolv-retry infinite
nobind
persist-key
persist-tun
remote-cert-tls server
auth SHA256
```

```
cipher AES-256-GCM
key-direction 1
verb 3

<ca>
-----BEGIN CERTIFICATE-----

-----END CERTIFICATE-----
</ca>
<cert>
-----BEGIN CERTIFICATE-----

-----END CERTIFICATE-----
</cert>
<key>
-----BEGIN PRIVATE KEY-----

-----END PRIVATE KEY-----
</key>
<tls-auth>
#
# 2048 bit OpenVPN static key
#
-----BEGIN OpenVPN Static key V1-----
-----END OpenVPN Static key V1-----
</tls-auth>
```

03 - Configuration du Routeur de Marseille

Building configuration...

Current configuration : 4294 bytes

!

version 12.4

service timestamps debug datetime msec

service timestamps log datetime msec

```
no service password-encryption
!
hostname RT-ITWAY05-MA
!
boot-start-marker
boot-end-marker
!
no logging buffered
enable password *****
!
no aaa new-model
ip cef
!
!
!
!
ip domain name 0870019y.lan
ip auth-proxy max-nodata-conns 3
ip admission max-nodata-conns 3
!
!
!
username btssio privilege 15 password 0 *****
username admin privilege 15 secret 5 *****
!
!
ip ssh time-out 60
ip ssh rsa keypair-name ssh
ip ssh version 2
!
!
```

```
!  
!  
interface FastEthernet0/0  
ip address 192.168.150.49 255.255.255.0  
ip nat outside  
ip virtual-reassembly  
duplex auto  
speed auto  
!  
interface FastEthernet0/1  
no ip address  
ip helper-address 192.168.100.10  
ip nat inside  
ip virtual-reassembly  
duplex auto  
speed auto  
!  
interface FastEthernet0/1.100  
encapsulation dot1Q 100  
ip address 192.168.100.1 255.255.255.240  
ip helper-address 192.168.100.10  
ip nat inside  
ip virtual-reassembly  
!  
interface FastEthernet0/1.110  
encapsulation dot1Q 110  
ip address 192.168.110.1 255.255.255.224  
ip helper-address 192.168.100.10  
ip nat inside  
ip virtual-reassembly  
!
```

```
interface FastEthernet0/1.120
encapsulation dot1Q 120
ip address 192.168.120.1 255.255.255.224
ip helper-address 192.168.100.10
ip nat inside
ip virtual-reassembly
!
interface FastEthernet0/1.130
encapsulation dot1Q 130
ip address 192.168.130.1 255.255.255.224
ip helper-address 192.168.100.10
ip nat inside
ip virtual-reassembly
!
interface FastEthernet0/1.140
encapsulation dot1Q 140
ip address 192.168.140.1 255.255.255.224
ip helper-address 192.168.100.10
ip nat inside
ip virtual-reassembly
!
interface FastEthernet0/1.150
!
interface FastEthernet0/1.160
encapsulation dot1Q 160
ip address 192.168.160.1 255.255.255.240
ip helper-address 192.168.100.10
ip nat inside
ip virtual-reassembly
!
interface FastEthernet0/1.170
```

```
encapsulation dot1Q 170
ip address 192.168.170.1 255.255.255.224
ip helper-address 192.168.100.10
ip nat inside
ip virtual-reassembly
!
interface FastEthernet0/1.500
encapsulation dot1Q 500
ip address 172.16.10.1 255.255.255.248
ip access-group ACL_FROM_DMZ in
ip access-group ACL_TO_PROXY out
ip nat inside
ip virtual-reassembly
!
router rip
version 2
network 172.16.0.0
network 192.168.100.0
network 192.168.110.0
network 192.168.120.0
network 192.168.130.0
network 192.168.140.0
network 192.168.150.0
network 192.168.160.0
network 192.168.170.0
no auto-summary
!
ip forward-protocol nd
ip route 0.0.0.0 0.0.0.0 192.168.150.1
ip route 172.16.20.0 255.255.255.248 192.168.100.11
ip route 192.168.200.0 255.255.255.240 192.168.100.11
```

```
ip route 192.168.210.0 255.255.255.240 192.168.100.11
ip route 192.168.220.0 255.255.255.240 192.168.100.11
ip route 192.168.230.0 255.255.255.240 192.168.100.11
!
!
no ip http server
no ip http secure-server
ip nat inside source list NAT_EXEMPT interface FastEthernet0/0 overload
ip nat inside source static udp 192.168.100.11 58803 interface FastEthernet0/0 58803
!
ip access-list extended ACL_FROM_DMZ
permit tcp any 172.16.10.0 0.0.0.7 established
permit tcp any 172.16.10.0 0.0.0.7 eq www
permit tcp any 172.16.10.0 0.0.0.7 eq 443
permit tcp any 172.16.10.0 0.0.0.7 eq 3128
permit ip 172.16.10.0 0.0.0.7 any
deny ip any any
ip access-list extended ACL_TO_PROXY
permit tcp any 172.16.10.0 0.0.0.7 established
permit tcp any 172.16.10.0 0.0.0.7 eq www
permit tcp any 172.16.10.0 0.0.0.7 eq 443
permit udp any 172.16.10.0 0.0.0.7
permit icmp any 172.16.10.0 0.0.0.7
permit tcp any 172.16.10.0 0.0.0.7 eq 22
permit tcp any host 172.16.10.2 eq 3128
deny ip any any log
ip access-list extended NAT_EXEMPT
permit ip 192.168.110.0 0.0.0.31 any
permit ip 192.168.120.0 0.0.0.31 any
permit ip 192.168.130.0 0.0.0.31 any
permit ip 192.168.140.0 0.0.0.31 any
```

```
permit ip 192.168.170.0 0.0.0.31 any
permit ip 172.16.10.0 0.0.0.7 any
permit ip 172.16.20.0 0.0.0.7 any
permit ip 192.168.100.0 0.0.0.15 any
permit ip 192.168.160.0 0.0.0.15 any
!
!
!
!
control-plane
!
!
!
line con 0
password *****
login
line aux 0
line vty 0 3
exec-timeout 5 0
login local
transport input ssh
line vty 4
exec-timeout 5 0
logging synchronous
login local
transport input ssh
!
scheduler allocate 20000 1000
end
```

04 Configuration du switch de Marseille

```
Current configuration : 3532 bytes
!
! Last configuration change at 19:44:57 UTC Mon Apr 27 2026 by admin
! NVRAM config last updated at 21:31:15 UTC Fri Apr 24 2026 by admin
!
version 15.0
no service pad
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname SW-ITWAY05-MA
!
boot-start-marker
boot-end-marker
!
enable password *****
!
username btssio password 0 *****
username admin privilege 15 secret 5*****
no aaa new-model
switch 1 provision ws-c2960x-24ps-l
!
!
ip domain-name 0870019y.lan
!
!
!
```

```
spanning-tree mode pvst
spanning-tree extend system-id
!
!
!
!
!
!
vlan internal allocation policy ascending
!
ip ssh time-out 60
ip ssh rsa keypair-name ssh
ip ssh version 2
!
!
!
!
!
interface Port-channel1
switchport trunk allowed vlan 100,110,120,130,140,150,160,170,500
switchport mode trunk
!
interface FastEthernet0
no ip address
!
interface GigabitEthernet1/0/1
switchport mode trunk
!
interface GigabitEthernet1/0/2
switchport access vlan 170
switchport mode access
```

```
shutdown
!
interface GigabitEthernet1/0/3
switchport access vlan 100
switchport mode access
!
interface GigabitEthernet1/0/4
switchport access vlan 100
switchport mode access
!
interface GigabitEthernet1/0/5
switchport access vlan 110
switchport mode access
!
interface GigabitEthernet1/0/6
switchport access vlan 110
switchport mode access
!
interface GigabitEthernet1/0/7
switchport access vlan 120
switchport mode access
!
interface GigabitEthernet1/0/8
switchport access vlan 120
switchport mode access
!
interface GigabitEthernet1/0/9
switchport access vlan 130
switchport mode access
!
interface GigabitEthernet1/0/10
```

```
switchport access vlan 130
switchport mode access
!
interface GigabitEthernet1/0/11
switchport access vlan 140
switchport mode access
!
interface GigabitEthernet1/0/12
switchport access vlan 140
switchport mode access
!
interface GigabitEthernet1/0/13
switchport access vlan 160
switchport mode access
!
interface GigabitEthernet1/0/14
switchport access vlan 160
switchport mode access
!
interface GigabitEthernet1/0/15
switchport access vlan 170
switchport mode access
!
interface GigabitEthernet1/0/16
switchport access vlan 170
switchport mode access
!
interface GigabitEthernet1/0/17
shutdown
!
interface GigabitEthernet1/0/18
```

```
shutdown
!
interface GigabitEthernet1/0/19
shutdown
!
interface GigabitEthernet1/0/20
shutdown
!
interface GigabitEthernet1/0/21
shutdown
!
interface GigabitEthernet1/0/22
shutdown
!
interface GigabitEthernet1/0/23
switchport trunk allowed vlan 100,110,120,130,140,150,160,170,500
switchport mode trunk
channel-group 1 mode active
!
interface GigabitEthernet1/0/24
switchport trunk allowed vlan 100,110,120,130,140,150,160,170,500
switchport mode trunk
channel-group 1 mode active
!
interface GigabitEthernet1/0/25
shutdown
!
interface GigabitEthernet1/0/26
shutdown
!
interface GigabitEthernet1/0/27
```

```
shutdown
!
interface GigabitEthernet1/0/28
!
interface Vlan1
no ip address
shutdown
!
interface Vlan100
ip address 192.168.100.2 255.255.255.240
!
interface Vlan170
no ip address
!
interface Vlan200
no ip address
!
interface Vlan500
no ip address
!
ip http server
ip http secure-server
!
!
!
banner motd ^CAcces autorise seulement au stagiaires et au administrateur ^C
!
line con 0
password *****
login
line vty 0 3
```

```
exec-timeout 5 0
login local
transport input ssh
line vty 4
exec-timeout 5 0
logging synchronous
login local
transport input ssh
line vty 5 15
login
!
end
```

05 Configuration du Switch de Lille

```
Building configuration...
```

```
Current configuration : 2869 bytes
```

```
!
```

```
! Last configuration change at 14:21:49 UTC Sun Apr 26 2026 by admin
```

```
! NVRAM config last updated at 21:42:07 UTC Fri Apr 24 2026 by admin
```

```
!
```

```
version 12.2
```

```
no service pad
```

```
service timestamps debug uptime
```

```
service timestamps log uptime
```

```
no service password-encryption
```

```
!
```

```
hostname SW-ITWAY05-LI
```

```
!
```

```
enable password *****
!
username btssio password 0
username admin privilege 15 secret 5
no aaa new-model
ip subnet-zero
!
ip domain-name 0870019y.lan
ip ssh time-out 60
ip ssh version 2
!
!
!
!
!
no file verify auto
spanning-tree mode pvst
spanning-tree extend system-id
!
vlan internal allocation policy ascending
!
interface Port-channel1
switchport trunk allowed vlan 200,210,220,230,240,600
switchport mode trunk
!
interface FastEthernet0/1
switchport trunk allowed vlan 200,210,220,230,240,600
switchport mode trunk
channel-group 1 mode active
!
interface FastEthernet0/2
```

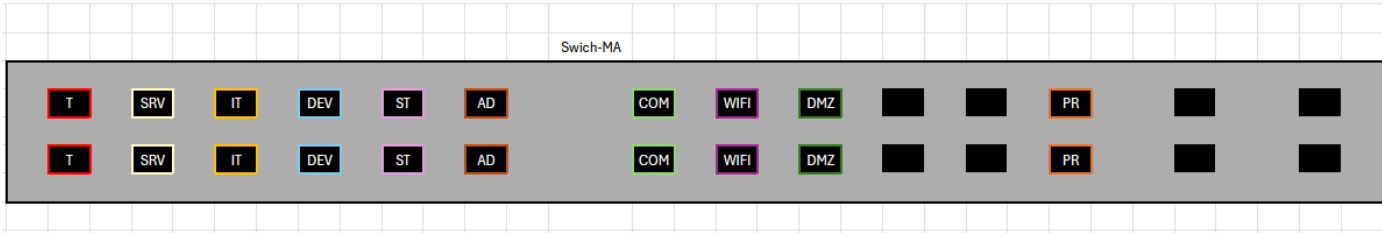
```
switchport trunk allowed vlan 200,210,220,230,240,600
switchport mode trunk
channel-group 1 mode active
!
interface FastEthernet0/3
switchport access vlan 200
switchport mode access
!
interface FastEthernet0/4
switchport access vlan 200
switchport mode access
!
interface FastEthernet0/5
switchport access vlan 210
switchport mode access
!
interface FastEthernet0/6
switchport access vlan 210
switchport mode access
!
interface FastEthernet0/7
switchport access vlan 220
switchport mode access
!
interface FastEthernet0/8
switchport access vlan 220
switchport mode access
!
interface FastEthernet0/9
switchport access vlan 230
switchport mode access
```

```
!  
interface FastEthernet0/10  
switchport access vlan 230  
switchport mode access  
!  
interface FastEthernet0/11  
switchport access vlan 600  
switchport mode access  
!  
interface FastEthernet0/12  
switchport access vlan 600  
switchport mode access  
!  
interface FastEthernet0/13  
shutdown  
!  
interface FastEthernet0/14  
shutdown  
!  
interface FastEthernet0/15  
shutdown  
!  
interface FastEthernet0/16  
shutdown  
!  
interface FastEthernet0/17  
shutdown  
!  
interface FastEthernet0/18  
shutdown  
!
```

```
interface FastEthernet0/19
shutdown
!
interface FastEthernet0/20
shutdown
!
interface FastEthernet0/21
shutdown
!
interface FastEthernet0/22
shutdown
!
interface FastEthernet0/23
shutdown
!
interface FastEthernet0/24
shutdown
!
interface GigabitEthernet0/1
shutdown
!
interface GigabitEthernet0/2
shutdown
!
interface Vlan1
no ip address
no ip route-cache
shutdown
!
interface Vlan200
ip address 192.168.200.2 255.255.255.240
```

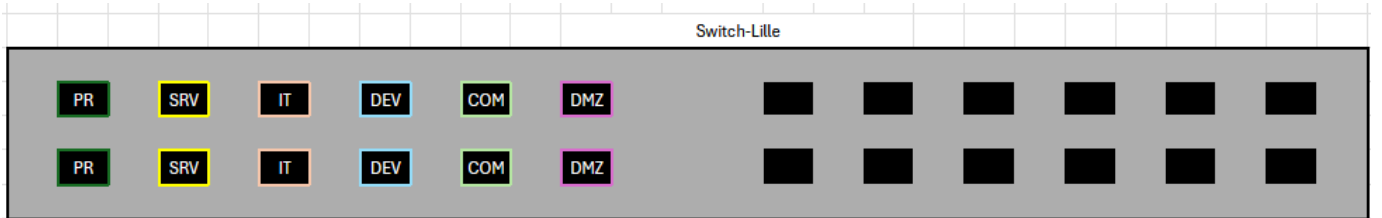
```
no ip route-cache
!
ip http server
ip http secure-server
!
control-plane
!
banner motd ^CAcces autorise seulement au stagiaires et au administrateur ^C
!
line con 0
password *****
login
line vty 0 3
exec-timeout 5 0
login local
transport input ssh
line vty 4
exec-timeout 5 0
logging synchronous
login local
transport input ssh
line vty 5 15
no login
!
end
```

06 – Ports switch Marseille



SIGNE	NOM	ID	RESEAU
T	TRUNK	100,110,120,130,140,160,170,500	N/A
PR	TRUNK +LACP	100,110,120,130,140,160,170,500	N/A
SRV	VLAN-MA-SRV	100	192.168.100.0
IT	VLAN-MA-IT	110	192.168.110.0
DEV	VLAN-MA-DEV	120	192.168.120.0
ST	VLAN-MA-ST	130	192.168.130.0
AD	VLAN-MA-AD	140	192.168.140.0
COM	VLAN-MA-COM	160	192.168.160.0
WIFI	VLAN-MA-WIFI	170	192.168.170.0
DMZ	VLAN-MA-DMZ	500	172.16.10.0

07 – Ports switch Lille



SIGNE	NOM	ID	RESEAU
PR	TRUNK	200,210,220,230,600	N/A
SRV	VLAN-LI-SRV	200	192.168.200.0
IT	VLAN-LI-IT	210	192.168.210.0
DEV	VLAN-LI-DEV	220	192.168.220.0
COM	VLAN-LI-COM	230	192.168.230.0
DMZ	Vlan-LI-DMZ	600	172.16.20.0

08-Utilisateurs de la Base de données (SBDG)

IP	PORT	DB NAME	USER	PASS	Service	Machine qui l'utilise
192.168.100.4	3306	wazuh_db	wazuh_user	btsSIO351	Wazuh	Serveur Wazuh
192.168.100.4	3306	Glipma_bd	GlpiMa_user	btsSIO351	glpi	Serveur GLPI
192,168,100,4	3306	guac_db	guac_user	btsSIO351	guacamole	Serveur Guacamole
192.168.100.4	3306	centreon	centreon	btsSIO351	Centreon	Serveur Centreon
192.168.100.4	3306	centreon_storage	centreon	btsSIO351		

09- Utilisateurs Active Directory

Marseille		Lille		Connecteurs	
Jordan Dupont	IT	Pierre Martin	Commercial	Sync-GLPI	Connecteur
Xavier Duchamp	IT	Henri Pierre	Commercial	mailuser	Connecteur
Louis Roux	IT	Monique Mercier	Commercial	guac	Connecteur
Louise Perez	IT	Olivier Petit	Développement logiciel	Centreon	Connecteur
matthias	IT	Claude Simon	Développement logiciel	Admin	Utilisateurs (Racine)
Lana Pavon	IT	Anne Gauthier	Développement logiciel		
Justine Fontaine	Commercial	Octave Lambert	Support Technique		
Julie Jean	Commercial	Paul Dubois	Support Technique		
Nicolas Durand	Commercial	Sylvie Renault	Support Technique		
Alain Jacquet	Commercial				
Élise Jean	Développement logiciel				
Roger Dominique	Développement logiciel				
Michel Fournier	Développement logiciel				
Robert Aubry	Développement logiciel				
John Doe	Support Technique				
Kevin Dumas	Support Technique				
Nathalie Bonnet	Support Technique				
Martine Dupuy	Support Technique				
Justin Bridou	Administratif				
Ambre Rousseau	Administratif				
Bernard Sanchez	Administratif				

10 - Tableau des services à déployer