

CAHIER DES CHARGES TECHNIQUE

AP3 - Appli Association



Sommaire :

1. Contexte.....	3
2. Objectif	4
3. Architecture cible & addressage IP	5
4. Autorisations et flux réseaux :	8
5. Création des UO Dans Active Directory.....	11
6. Base de données.....	12
7. Proxmox et ses VM / Conteneurs	14
8. Proxmox Backup Server	15

1. Contexte

Notre établissement, le lycée Pasteur Mont-Roland situé dans la ville de Dole, organise annuellement des journées santé et citoyenneté.

En cette occasion, plusieurs personnes interviennent : des élèves de seconde et première année, des associations, la police, la sécurité routière etc...

Mais le lycée rencontre un problème : la gestion de ces journées repose sur des échanges de mails, de documents, et n'est pas centralisée, ni automatisée, ce qui est chronophage en plus de présenter un risque d'erreurs, de perte d'information, etc...

M. PERNELLE Sébastien, notre professeur, nous invite donc à mettre en place dans le cadre de notre 3ème projet d'atelier professionnel, une solution permettant de répondre à ce besoin de simplification et de centralisation de gestion.

Les BTS SIO – Option SLAM (Solution logicielles et applications métier) travailleront donc en collaboration avec leurs camarades en Option SISR (Solution d'infrastructure, systèmes et réseaux) afin de mener à bien ce projet.

2. Objectif

Ainsi, le but a été défini : permettre à un administrateur d'envoyer des invitations aux associations via une interface de gestion centralisée.

Pour cela, deux applications seront créées :

- **Une application lourde**, hébergée sur notre serveur Windows, dont nous permettront l'accès à M. Pernelle via un système de bureau à distance, ou il pourra gérer les invitations
- **Une application web**, hébergée sur notre serveur web et accessible par les associations. Ces dernières pourront choisir si elles le souhaitent de s'inscrire à la journée santé et citoyenneté via une interface web.

Le formulaire présent sur cette interface contiendra différents champs, comme :

- Titre de l'activité
- Détail de l'activité
- Date et horaires
- Identité de l'intervenant
- Besoin matériels
- Tarifs de l'intervention

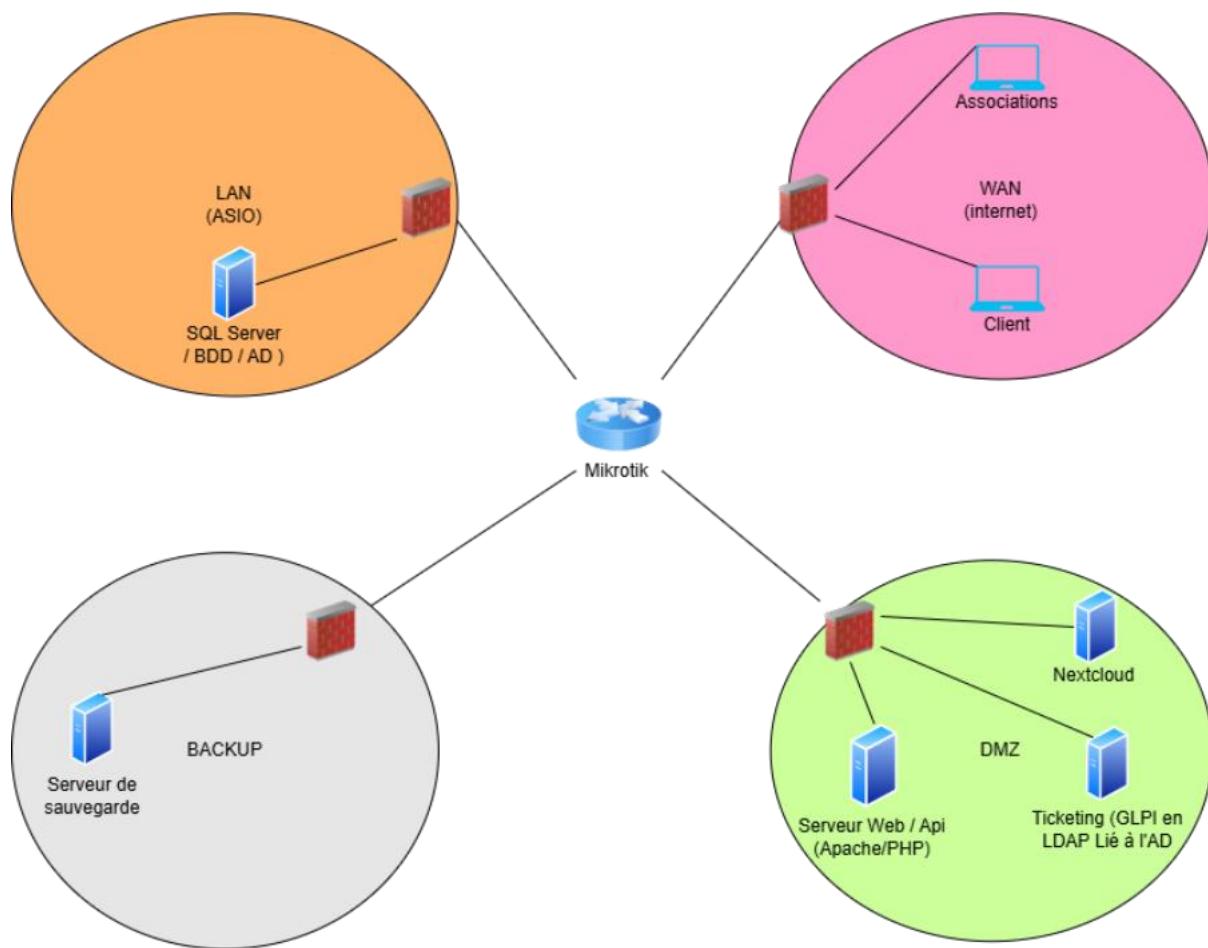
Les informations saisies seront ensuite transmises à l'application lourde, qui s'occupera de les stocker dans la base de données SQL Server, elle aussi sur notre serveur Windows.

Dans ce contexte, notre objectif à nous, en spécialité SISR (solution d'infrastructure, système & réseaux), est de **mettre en place l'infrastructure réseau permettant d'accueillir ces deux applications.**

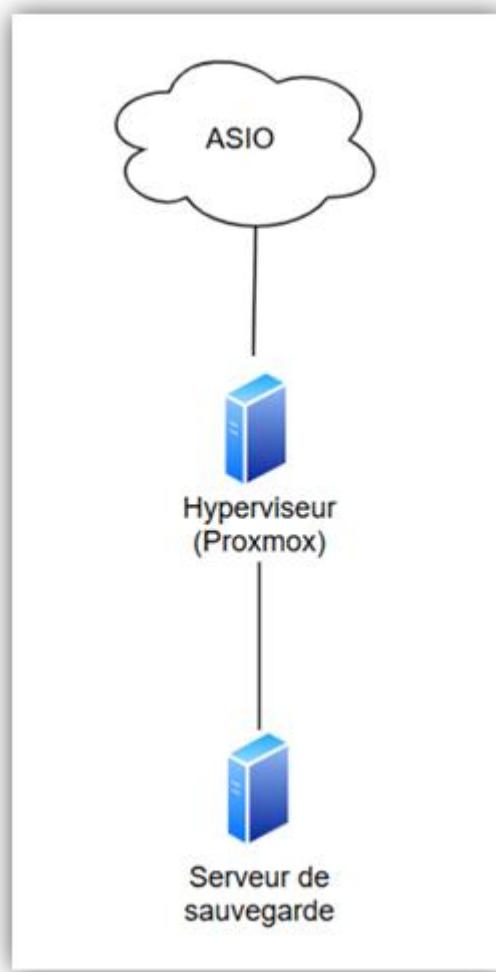
3. Architecture cible & addressage IP

Pour une meilleure visualisation de ce projet, nous avons établis 2 schémas : un schéma logique et un physique.

- **3.1 Schéma logique :**



3.2 Schéma physique :



3.3 Plan d'adressage IP :

Nos sous-réseaux sont organisés de la façon suivante :

Lycée Pasteur Mont
Roland – Dole.

DOS SANTOS Dylan
GRUET Léo
MORBOEUF Evan

**BTS Service
Informatiques aux
Organisations**

Année 2025-2026

172.20.4.31/16		
WAN	NOM MACHINE	ADRESSE IP
	Proxmox	172.20.14.30
	Mikrotik	172.20.14.31

192.168.50.254/24		
LAN	NOM MACHINE	ADRESSE IP
	Windows Server	192.168.50.1

192.168.52.254/24		
BACKUP	NOM MACHINE	ADRESSE IP
	Proxmox backup server	172.20.14.32

192.168.51.254/24		
DMZ	NOM MACHINE	ADRESSE IP
	Nextcloud	192.168.51.2 /25
	Gipi	192.168.51.3 /25
	Serveur web	192.168.51.1 /24

4. Autorisations et flux réseaux :

Pour établir les **règles de notre pare-feu**, nous nous sommes basés sur le principe du **moindre privilège** et la **protection des données** dites " critiques ".

4.1 Règles de filtrage :

Filter Rules													NAT	Mangle	Raw	Service Ports	Connections	Address Lists	Layer7 Protocols
#	Action	Chain	Src. Address	Dst. Address	Src. Ad.	Dst. Ad.	Proto	Src. Port	Dst. Port	In. Interf.	Out. Inte...	In. Interf.	Out. Inte...	Bytes	Packets				
0	green checkmark acc... forward	ENABLE ESTABLISHED CONNEXIONS												34950 MiB	1 836 060				
1	green checkmark acc... forward	ENABLE PING					1 (icmp)							0 B	0				
2	green checkmark acc... forward	ENABLE DST SERVEUR-WEB		192.168.51.1			6 (tcp)	80						1691 B	34				
3	green checkmark acc... forward	ENABLE DST NEXT-CLOUD		192.168.51.2			6 (tcp)	80						5.1 kB	101				
4	green checkmark acc... forward	ENABLE DST GLPI		192.168.51.3			6 (tcp)	80						717 B	14				
5	green checkmark acc... forward	ENABLE SW TO WINDOWS-SERVER(BDD)		192.168.51.1	192.168.50.1		6 (tcp)	1433						1380 B	23				
6	green checkmark acc... forward	ENABLE SW TO WINDOWS-SERVER(dap nextcloud)		192.168.51.2	192.168.50.1		6 (tcp)	389						8.3 kB	141				
7	green checkmark acc... forward	ENABLE SW TO WINDOWS-SERVER(glpi)		192.168.51.3	192.168.50.1		6 (tcp)	389						120 B	2				
8	green checkmark acc... forward	ENABLE SW TO WINDOWS-SERVER(RDP)		192.168.50.1			6 (tcp)	3389						416 B	8				
9	green checkmark acc... forward			192.168.51.1			6 (tcp)	22						312 B	6				
10	red crossed-out drop	DROP OTHERS CONNEXIONS	forward											9.3 MiB	144 560				

Ainsi, nous avons établis les règles suivantes :

0. Autorise le retour des paquets pour les connexions déjà validées afin de fluidifier le trafic.
1. (PING) : Permet d'utiliser la commande ping pour diagnostiquer la connectivité entre les réseaux.
2. (SERVEUR-WEB) : Ouvre l'accès au port HTTP (80) pour le serveur web hébergeant l'application web.
3. (NEXTCLOUD) : Autorise l'accès à l'interface de stockage cloud pour la gestion des logos des associations.

4. (GLPI) : Permet l'accès à l'outil de gestion de parc et de tickets (GLPI) via le port web.

5. (SQL SERVER) : Autorise uniquement le serveur web à interroger la base de données sur le port 1433.

6. (LDAP NEXTCLOUD) : Permet à Nextcloud de vérifier les identifiants des utilisateurs auprès de l'Active Directory.

7. (LDAP GLPI) : Permet à GLPI de s'appuyer sur l'annuaire Windows pour l'authentification des comptes.

8. (RDP) : Autorise le contrôle à distance du serveur Windows pour l'administrateur via le port 3389.

9. (SSH) : Permet l'administration sécurisée en ligne de commande du serveur web sur le port 22.

10 (DROP OTHERS) : Bloque par sécurité toute tentative de communication n'ayant pas été explicitement autorisée plus haut.

4.2 Règles NAT (Network Address Translation)

Pour permettre l'accès au sous-réseau de notre projet depuis le réseau du lycée, nous avons mis en place plusieurs règles NAT.

Firewall															
Filter Rules NAT Mangle Raw Service Ports Connections Address Lists Layer7 Protocols															
#	Action	Chain	Src. Address	Dst. Address	Src. Ad...	Dst. Ad...	Proto...	Src. Port	Dst. Port	In. Inter...	Out. Int...	In. Inter...	Out. Int...	Bytes	Packets
0	.masquerade	srcnat												1148 B	18
	... redirection vers 192.168.50.1 (SRV-AD-BDD)														
1	.* dst-nat	dstnat		172.20.14.31			6 (tcp)		3389					832 B	16
	... redirection vers 192.168.51.1 (SRV-WEB)														
2	.* dst-nat	dstnat		172.20.14.31			6 (tcp)		8080					1743 B	35
	... redirection 192.168.51.1 (SRV-WEB)														
3	.* dst-nat	dstnat		172.20.14.31			6 (tcp)		2222					312 B	6
	... redirection 192.168.50.1 (SRV-AD-BDD)														
4	.* dst-nat	dstnat		172.20.14.31			6 (tcp)		1433					708 B	13
	... redirection 192.168.51.3 (SRV-GLPI)														
5	.* dst-nat	dstnat		172.20.14.31			6 (tcp)		8081					1828 B	36
	... redirection vers 192.168.51.2 (SRV-NEXTCLOUD)														
6	.* dst-nat	dstnat		172.20.14.31			6 (tcp)		8082					5.1 KiB	101

0 (masquerade) : Permet à tous tes équipements du labo de partager l'adresse IP du routeur pour accéder à Internet via l'interface ether1, et que le retour puisse avoir lieu.

1 (RDP vers BDD) : Redirige le trafic arrivant sur le port 3389 vers le serveur Windows (192.168.50.1) pour l'administration à distance.

2 (HTTP vers WEB) : Redirige les requêtes web du port 8080 vers le serveur web (192.168.51.1).

3 (SSH vers WEB) : Permet d'administrer le serveur web en ligne de commande via le port déporté 2222.

4 (SQL vers BDD) : Redirige les flux de données du port 1433 vers le serveur de base de données SQL Server.

5 (HTTP vers GLPI) : Permet d'accéder à l'interface de gestion de parc GLPI via le port 8081.

6 (HTTP vers NEXTCLOUD) : Redirige le trafic du port 8082 vers l'instance Nextcloud pour la gestion des fichiers.

5. Crédation des UO Dans Active Directory

Nous avons créé une unité d'organisation **IT**, contenant deux autres UO, une pour les **développeurs** et une pour les **réseaux**.

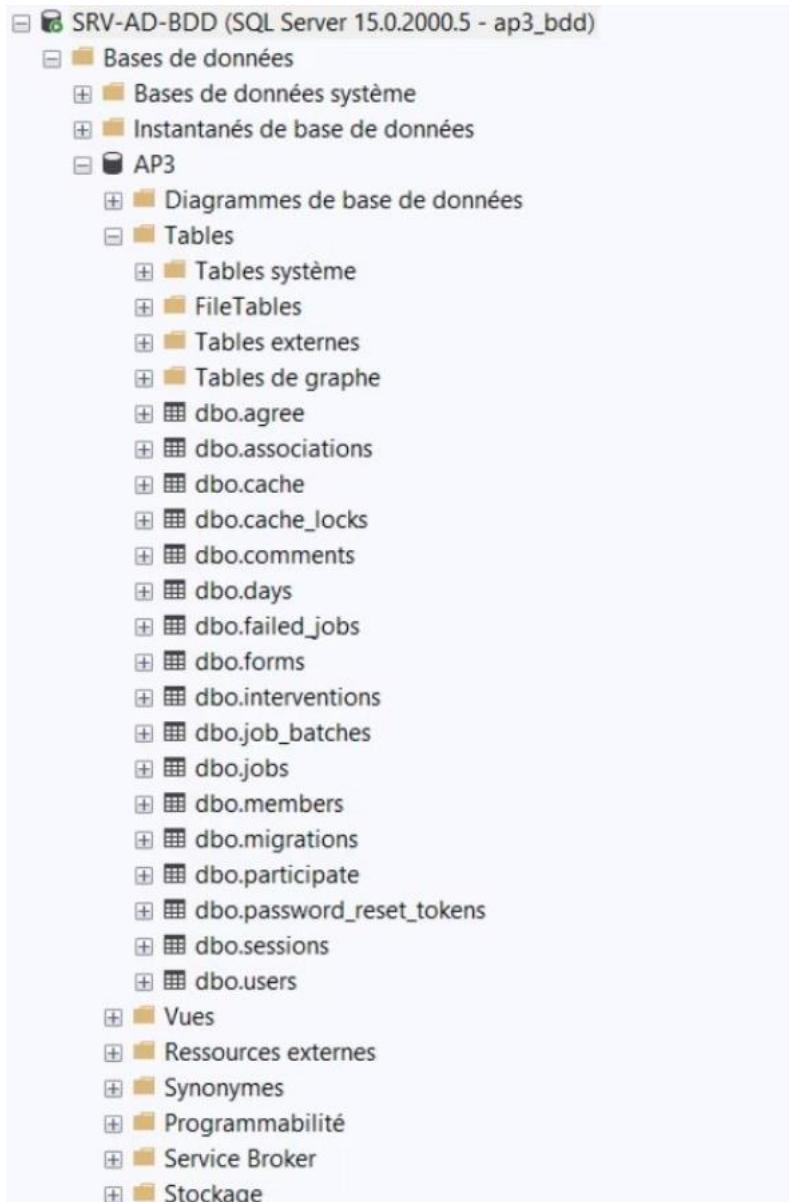
Nous avons également créé un utilisateur dédié à la **BDD**, ainsi qu'un à **Nextcloud**, ces deux comptes respectant le principe du “ **moindre privilège** ”, ils font quelque part office de “ compte bot ”.

AP3 BDD permet au SW de lire la BDD, et nextcloud permet à notre Nextcloud de lire la BDD.

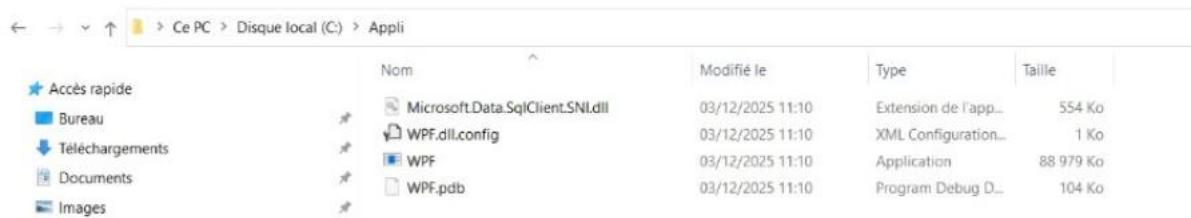
Utilisateurs et ordinateurs Active Directory [SRV]	Nom	Type	Description
Requêtes enregistrées	DEV	Unité d'organis...	
groupe2.local	RESEAU	Unité d'organis...	
BuiltIn	AP3 BDD	Utilisateur	
Computers	nextcloud	Utilisateur	
Domain Controllers			
ForeignSecurityPrincipals			
Keys			
LDAP			
LostAndFound			
Managed Service Accounts			
Program Data			
Project			
Computers			
IT			
DEV			
RESEAU			
Users			
System			
Users			
NTDS Quotas			
TPM Devices			

6. Base de données

Voici les différentes tables créées par le script de nos camarades SLAM.



Également l'emplacement de l'application lourde :



A screenshot of a Windows File Explorer window. The path is Ce PC > Disque local (C) > Appli. The table lists the following files:

	Nom	Modifié le	Type	Taille
	Microsoft.Data.SqlClient.SNI.dll	03/12/2025 11:10	Extension de l'app...	554 Ko
	WPF.dll.config	03/12/2025 11:10	XML Configuration...	1 Ko
	WPF	03/12/2025 11:10	Application	88 979 Ko
	WPF.pdb	03/12/2025 11:10	Program Debug D...	104 Ko

7. Proxmox et ses VM / Conteneurs

Comme prévu, nous retrouvons sur notre hyperviseur nos VM et conteneurs.

The screenshot shows the Proxmox VE 9.0.3 interface. On the left, there's a tree view of the datacenter named 'pve' containing several virtual machines and containers. A search bar at the top right shows 'Node "pve"'. Below it, a toolbar has buttons for 'Documentation', 'Create VM', 'Create CT', and 'root@pve'. The main area is a table listing resources:

Type	Description	Disk usage...	Memory us...	CPU usage	Uptime	Host CPU ...	Host ...
lxc	101 (SRV-NEXTCLOUD)	4.1 %	9.8 %	0.0% of 2 ...	62 days 23:3...	0.0% of 8 ...	0.6 %
lxc	103 (SRV-GLPI)	10.4 %	16.3 %	0.0% of 2 ...	63 days 03:0...	0.0% of 8 ...	1.0 %
lxc	104 (SRV-WEB)	62.3 %	32.8 %	0.0% of 1 ...	40 days 20:4...	0.0% of 8 ...	0.5 %
qemu	100 (Routeur-Mikrotik)	0.0 %	50.8 %	1.2% of 2 ...	83 days 00:4...	0.3% of 8 ...	1.6 %
qemu	102 (WINDOWS-SERVER-2022)	0.0 %	66.5 %	2.4% of 4 ...	83 days 00:2...	1.2% of 8 ...	25.8 %
sdn	localnetwork (pve)	-	-	-	-	-	-
storage	local (pve)	18.3 %	-	-	-	-	-
storage	local-lvm (pve)	35.0 %	-	-	-	-	-

Nous avons privilégié les containers afin d'**optimiser les ressources** de notre hyperviseur. En revanche, le cœur de réseau (MikroTik) et Windows étant des système propriétaires avec leurs propres OS, nous avons utilisé des VM.

8. Proxmox Backup Server

Pour notre solution de sauvegarde automatisée, nous avons paramétré une sauvegarde hebdomadaire, avec une conservation des 5 dernières sauvegardes.

The screenshot shows the Proxmox Backup Server 4.1.0 interface. The left sidebar contains navigation links for Dashboard, Notes, Configuration, Remotes, S3 Endpoints, Traffic Control, Certificates, Notifications, Subscription, Administration, Shelf, Storage / Disks, Tape Backup, and Datastore. The main area displays system statistics for 'SRV-BACKUP' (Uptime: 33 days 22:39:21) including CPU usage (2.39% of 4 CPU(s)), RAM usage (12.82% of 490.20 MB of 3.74 GiB), HD space (root: 1.44% of 3.19 GB of 221.86 GB), and Swap usage (0.00% of 0 B of 4.00 GiB). It also shows hardware details: 4 x Intel(R) Core(TM) i3-2100 CPU @ 3.10GHz (1 Socket), Linux 6.17.2-1.pve (2025-10-21T11:55Z), Legacy BIOS, and a note about a production-ready enterprise repository. Below this is a 'Datastore Usage' table:

Name	Size	Used	Available	Usage %	Estimated Full	History (last Month)
backups	210.52 GB	3.19 GB	207.33 GB	1.52%	in 689y 200d 18h	