Dossier d’Architecture Technique (DAT) — Smart Office 2.0

1. Contexte et objectifs

1.1. Contexte métier, effectifs, croissance, contraintes temporelles

Le projet s'inscrit dans le cadre du déménagement du siège social d'une startup en biotechnologie en situation d'hyper-croissance.

• **Évolution des effectifs** : Passage de 50 à 200+ collaborateurs sous 18 mois.

• **Mode de travail** : Hybride (jusqu'à 3 jours de télétravail/semaine), nécessitant des accès distants sécurisés.

• **Enjeu critique** : L'infrastructure doit être redondante et évolutive ("Scalable") pour absorber la charge sans refonte majeure.

1.2. Objectifs techniques et périmètre

L'objectif est de livrer une infrastructure "clés en main" respectant les standards de l'état de l'art :

• **Sécurité** : Approche "Zero Trust" (vérification systématique) et segmentation réseau stricte.

• **Haute Disponibilité** : Tolérance aux pannes matérielles (Cœur de réseau redondant) et liens WAN secourus.

• **Modernité** : Approche hybride Cloud/On-Premise et déploiement applicatif conteneurisé.

2. Exigences et contraintes

2.1. Fonctionnelles (télétravail, disponibilité)

2.2. Non fonctionnelles (sécu, perf, coût, scalabilité)

2.3. Contraintes budget simulé, calendrier (Déc 2025–Avr 2026, 6 séances)

3. Architecture réseau

3.1. Schéma physique (core/distribution/access, WAN primaire/backup, DMZ)

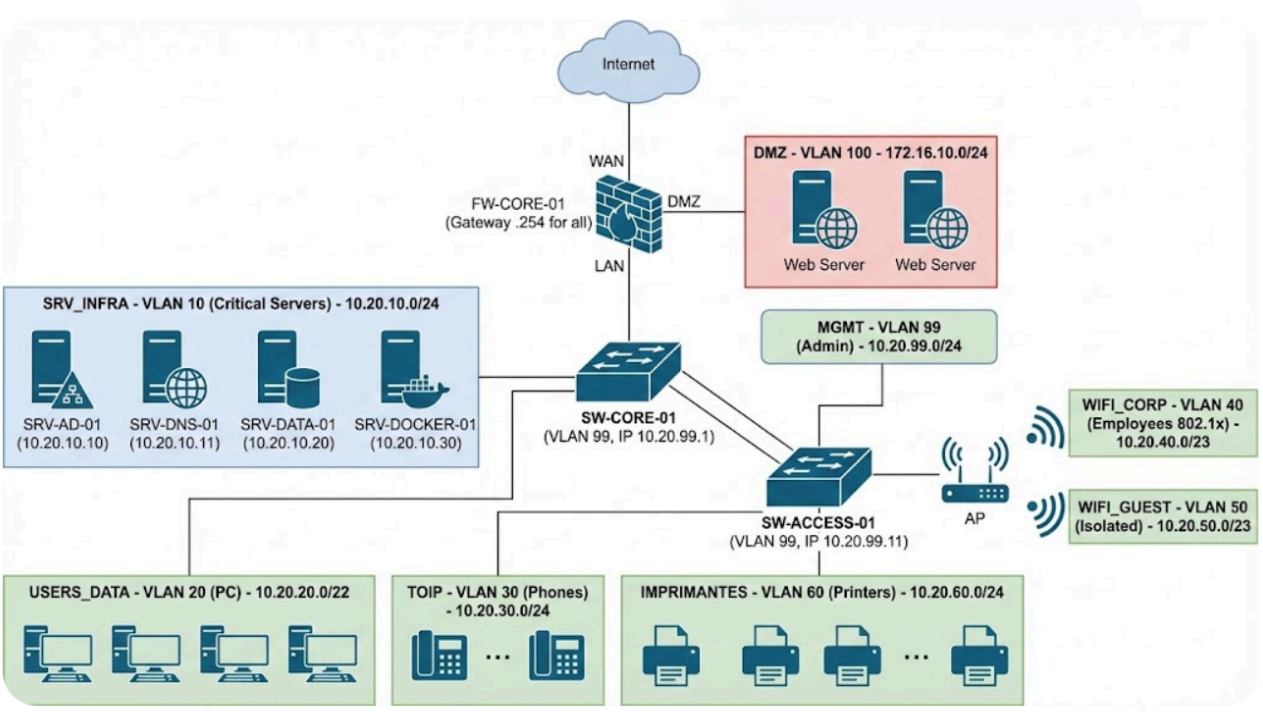

Figure 1: Architecture Globale (Physique et Logique)

L'architecture physique du siège social (4 étages) repose sur un modèle hiérarchique compressé dit "**Collapsed Core**". Ce choix est justifié par la taille de l'infrastructure (< 500 ports) : il permet de réduire la latence, simplifier la gestion et optimiser le budget (TCO) en fusionnant les couches "Cœur" et "Distribution".

Détail des équipements et justifications :

• **Nœud de Sécurité (Edge / Périmètre) :**
◦ Équipement : Pare-feu de Nouvelle Génération (NGFW) – Modèle simulé : PFsense/Fortigate.
◦ Rôle : Il assure la terminaison des liens WAN, le routage vers Internet, la terminaison des tunnels VPN et l'inspection profonde des paquets (IPS/IDS).

◦ Justification : Indispensable pour garantir la sécurité périmétrique et la segmentation stricte entre la zone DMZ, le LAN et le WAN (Zero Trust).

• **Cœur de Réseau (Core) :**
◦ Équipement : Switch de Niveau 3 (L3).
◦ **Redondance (Exigence de Haute Disponibilité)** : En production cible, ce cœur est constitué de **deux switchs physiques en stack (empilement)** ou configurés en vPC/VSS. Cela garantit qu'une panne matérielle d'un switch n'interrompt pas le service.
◦ Rôle : Routage inter-VLAN haute performance et application des ACLs internes.

• **Couche Accès (Access - Étages 1 à 4)** :
◦ Équipement : Switchs de Niveau 2 (L2) PoE+ (Power over Ethernet).
◦ Rôle : Raccordement des terminaux utilisateurs (PC), des téléphones IP (ToIP) et des bornes Wi-Fi.
◦ Liaisons : Chaque switch d'accès est relié au cœur par des liens agrégés (LACP / Etherchannel) pour augmenter la bande passante et assurer la résilience en cas de coupure d'un câble.

• **Connectivité WAN (Internet)** :
◦ Lien Principal : Fibre optique dédiée (Garantie de temps de Rétablissement - GTR 4h) pour le trafic critique.
◦ Lien de Secours (Failover) : Liaison 4G/5G ou VDSL. Le pare-feu est configuré pour basculer automatiquement (SD-WAN/Failover) sur ce lien en cas de perte de la fibre principale, assurant la continuité d'activité.
• Infrastructure Serveurs (Virtualisation) :
◦ Les serveurs (Contrôleur de domaine, DNS, Fichiers, Docker) sont virtualisés sur un hyperviseur de Type 1, relié au cœur de réseau via des liens 10Gbps (VLAN 10 - Server Farm).

3.2. Schéma logique (VLANs, sous-réseaux, routage, QoS)

Principes de segmentation (VLANs) : L'architecture logique repose sur une segmentation stricte par usage (VLANs) plutôt que par géographie. Cette approche permet d'appliquer des politiques de sécurité granulaires quel que soit l'endroit où l'utilisateur se connecte dans le bâtiment (Siège sur 4 étages).
• Voir le détail des ID VLANs dans la section *3.3 Plan d'adressage*.
• Le trafic "Invité" (VLAN 50) est totalement isolé du trafic de production (VLAN 20) dès la couche accès.

Stratégie de Routage (Inter-VLAN) :

• **Routage Interne (LAN)** : Le routage entre les différents VLANs (ex: PC vers Imprimante) est effectué par le **Cœur de Réseau (Switch L3)**. Cela permet de traiter le trafic à la vitesse du câble (Wire-speed) sans surcharger le pare-feu pour les flux internes de confiance.

• **Routage de sortie (WAN/DMZ)** : Tout trafic destiné à Internet ou sortant vers la DMZ est redirigé vers le **Pare-feu (Gateway)** via une route par défaut. Le pare-feu inspecte ces flux (Stateful Inspection).

Qualité de Service (QoS) : Afin de garantir la fluidité des communications (exigence critique du cahier des charges), une politique de QoS est appliquée sur les switchs :

1. **Classe "Priorité Haute" (Voice)** : Le VLAN 30 (ToIP) est marqué avec la valeur DSCP EF (Expedited Forwarding) / CoS 5. Il est prioritaire sur tous les liens, garantissant l'absence de gigue (jitter) pour les appels téléphoniques.
2. **Classe "Best Effort"** : Les données utilisateurs (VLAN 20) et le Wi-Fi (VLAN 40) utilisent la bande passante restante.
3. **Classe "Scavenger" (Basse priorité)** : Le trafic Wi-Fi Invité (VLAN 50) est limité en bande passante (Rate Limiting) pour ne jamais impacter la production.

3.3. Plan d'adressage IPv4/IPv6, DHCP, DNS

Le plan d'adressage a été conçu pour garantir la scalabilité (croissance future > de **50 à 200+ employés en 18 mois**) et la sécurité par segmentation (VLANs dédiés). Nous utilisons un **adressage privé** (10.x.x.x) découpé en sous-réseaux /22 /23 et /24.

VLAN ID	Nom du VLAN	Description	Réseau (CIDR)	Masque	Passerelle (Gateway)	Plage DHCP
10	SRV_INFRA	Serveurs Critiques (AD, DNS, DHCP)	10.20.10.0 /24	255.255.255.0	10.20.10.254	Statique uniquement
20	USERS_DATA	Postes de travail (PC)	10.20.20.0 /22	255.255.252.0	10.20.23.254	10.20.20.10 - 10.20.23.250
30	TOIP	Téléphonie IP	10.20.30.0 /23	255.255.254.0	10.20.31.254	10.20.30.10 - 10.20.31.250
40	WIFI_CORP	Wi-Fi Employés (Authentifiés 802.1x)	10.20.40.0 /23	255.255.254.0	10.20.41.254	10.20.40.10 - 10.20.41.250
50	WIFI_GUEST	Wi-Fi Invités (Isolé, portail captif)	10.20.50.0 /23	255.255.254.0	10.20.50.254	10.20.50.10 - 10.20.51.250
60	IMPRIMANTES	Imprimantes réseaux	10.20.60.0 /24	255.255.255.0	10.20.60.254	Réservations DHCP
99	MGMT	Administration Switchs/Routeurs	10.20.99.0 /24	255.255.255.0	10.20.99.254	Statique
100	DMZ	Zone Démilitarisée (Services Web)	172.16.10.0 /24	255.255.255.0	172.16.10.254	Statique

Inventaire des IPs statiques:

Rôle	Nom machine (Hostname)	VLAN	Adresse IP	Pourquoi ?
Pare-feu (Gateway)	FW-CORE-01	Tous	10.20.xx.254	C'est la passerelle par défaut de chaque VLAN.
Contrôleur de Domaine	SRV-AD-01	10	10.20.10.10	Le cœur de l'authentification (Active Directory).
Serveur DNS	SRV-DNS-01	10	10.20.10.11	Souvent le même que l'AD, mais note l'IP.
Serveur Fichiers	SRV-DATA-01	10	10.20.10.20	Pour les partages réseau.

Serveur App (Docker)	SRV-DOCKER-01	10	10.20.10.30	Là où tu mettras ton appli de réservation.
Switch Cœur	SW-CORE-01	99	10.20.99.1	Pour administrer le switch à distance (SSH).
Switch Etage 1	SW-ACCESS-01	99	10.20.99.11	Pour administrer le switch à distance (SSH).

3.4. Wi-Fi (SSID, segmentation, sécurité)

3.5. Flux réseau clés (app, DB, admin)

4. Sécurité

4.1. Segmentation (VLANs, DMZ), ACLs, pare-feu (règles)

Stratégie de Défense en Profondeur : La sécurité ne repose pas uniquement sur le périmètre, mais sur une segmentation interne stricte :

1. **Principe du moindre privilège** : Par défaut, tout le trafic inter-VLAN est bloqué ("**Deny All**"). Seuls les flux explicitement autorisés (ex: PC vers Imprimante) sont ouverts.

2. **Cloisonnement de la DMZ** : La DMZ (VLAN 100) n'a aucun accès au réseau interne (LAN). Elle ne peut qu'être contactée depuis l'extérieur (Internet) ou répondre à des requêtes spécifiques du LAN.

3. **Protection du Management** : Les interfaces d'administration (SSH/HTTPS) des switchs et pare-feu sont accessibles uniquement depuis le VLAN 99 ou via un VPN administrateur dédié.

4.2. Accès distants (VPN + MFA), NAC / Zero Trust (posture, identité)

4.3. Bastion / Jump host, gestion des comptes et secrets

4.4. Journalisation, SIEM, alerting

5. Infrastructure Cloud & Systèmes

5.1. Choix cloud, TCO et modèle hybride

5.1.1. Stratégie d'hybridation

L'infrastructure de Smart Office 2.0 repose sur un modèle hybride. Ce choix permet de conjuguer la sécurité et le contrôle d'une infrastructure locale avec la flexibilité et

l'évolutivité du Cloud public, indispensables pour soutenir la croissance prévue de 50 à plus de 200 collaborateurs en 18 mois.

On-Premise (Local) : Hébergement des services nécessitant une faible latence et un contrôle absolu de la donnée (Contrôleur de domaine AD, serveurs de fichiers, DNS local).

Cloud Public : Hébergement des services web exposés à l'extérieur (application de réservation de salles) et stockage des externalisations de sauvegardes pour le PRA.

5.1.2. Comparatif des fournisseurs Cloud et justification

Une analyse des trois acteurs majeurs du marché (AWS, Azure, GCP) a été menée.

AWS (Amazon Web Services) : Leader du marché, propose une offre pléthorique et robuste. Cependant, l'intégration avec un annuaire Active Directory On-Premise nécessite des configurations tierces plus complexes.

GCP (Google Cloud Platform) : Très performant sur la donnée et l'orchestration de conteneurs (Kubernetes natif). Moins pertinent pour un environnement bureautique et identitaire centré sur l'écosystème Microsoft.

Microsoft Azure : Offre une intégration native et transparente avec l'Active Directory local via Azure AD Connect (Entra ID).

Choix retenu : Microsoft Azure. Ce choix est justifié par le besoin de centraliser la gestion des identités (IAM) pour appliquer efficacement les principes du **Zero Trust** et du **MFA** exigés par le cahier des charges. De plus, Azure offre des solutions **PaaS très optimisées** pour le déploiement de **conteneurs Docker**.

5.1.3. Modèle de service : Le choix du PaaS

Pour l'application de réservation de salles conteneurisée, nous optons pour un modèle PaaS (Platform as a Service) via **Azure Container Apps**, plutôt qu'une machine virtuelle classique (IaaS).

Avantages opérationnels : Aucune gestion de l'OS sous-jacent (patching, mises à jour de sécurité). L'équipe IT se concentre uniquement sur le déploiement du conteneur (approche DevOps).

Scalabilité : Le service PaaS s'adapte automatiquement (Auto-scaling) à la charge. Si de nombreux employés réservent des salles simultanément, l'infrastructure s'étend sans intervention manuelle.

5.1.4. Analyse du TCO (Total Cost of Ownership) sur 3 ans

Cette simulation financière démontre l'intérêt du modèle PaaS Cloud face à un hébergement On-Premise strict pour notre application web métier.

Scénario A : Hébergement de l'application On-Premise (IaaS physique)

Achat d'un serveur physique dédié (CAPEX) : 3 500 €

Licences (Hyperviseur, OS) sur 3 ans : 1 200 €

Frais d'exploitation (OPEX) : Électricité, refroidissement, maintenance matérielle, temps homme pour le patching OS (estimé à 150 €/mois) : 5 400 € sur 3 ans.

TCO estimé sur 3 ans (On-Premise) : ~ 10 100 €

Scénario B : Hébergement Cloud (Azure Container Apps - PaaS)

Investissement de départ (CAPEX) : 0 €

Coût de calcul et bande passante (OPEX) : Modèle "Pay-As-You-Go", dimensionné pour un usage aux heures de bureau (estimé à 40 €/mois) : 1 440 € sur 3 ans.

Temps d'administration réduit (NoOps OS) : 0 € de frais cachés de maintenance.

TCO estimé sur 3 ans (Cloud PaaS) : ~ 1 440 €

Conclusion du TCO : Le choix de l'hybridation avec le PaaS Azure permet de diviser les coûts d'hébergement de l'application par sept sur une période de 3 ans, tout en garantissant une haute disponibilité et une tolérance aux pannes supérieures à un serveur local unique.

5.2. Services déployés (IaaS/PaaS), réseau cloud (VNet/VPC, peering/VPN)

5.3. Images, durcissement, patch management

6. Stockage et Bases de Données

6.1. Besoins (fichiers, sauvegardes, logs), choix SAN/NAS/Objet

6.2. Modèle de données (app POC), DB (SQL/NoSQL), HA/backup/restore

6.3. Sécurité DB (comptes, chiffrement, audit)

7. DevOps, Containerisation et CI/CD

7.1. Docker/compose, registre (GHCR), pipeline CI (build/test/push)

7.2. Déploiement cloud (K8s ou service managé / VM), IaC (Terraform)

7.3. Runbooks de déploiement

8. Supervision, Logs et Détection

8.1. Stack (ELK/Graylog, Grafana/Prometheus)

8.2. Sources (FW, app, système), tableaux de bord, alertes

8.3. Scénario d'anomalie simulée

9. PCA / PRA et ITSM

9.1. BIA, RTO/RPO par service

9.2. Scénarios (panne FAI, cyberattaque, panne serveur)

9.3. Procédures PRA/PCA, tests, rôles

9.4. Processus incidents (ticketing, escalade, SLA)

10. Gestion de projet et traçabilité

10.1. Méthode (Scrum), sprints, jalons

Le projet est piloté selon le framework Scrum, découpé en **Sprints** de 1 à 2 semaines.

• **Rituels** : Daily Stand-up (point rapide), Sprint Planning et Rétrospective.

• **Suivi** : Un tableau Kanban (Jira) permet de visualiser le flux de travail (To Do / In Progress / Done).

10.2. Outils collaboratifs et Qualité

• **Versionning (Git/GitHub)** : L'intégralité du code (IaC, scripts) et de la documentation est versionnée. Chaque fonctionnalité fait l'objet d'une branche dédiée et d'une Pull Request (PR) pour validation avant fusion.

• **Documentation** : Rédaction au fil de l'eau (Notion/Markdown) centralisée dans ce DAT.

10.3. Journal de décisions

11. Budget/TCO (simulé)

11.1. Estimation POC mensuelle cloud

11.2. Comparatif On-Prem vs Cloud (3 ans)

12. Annexes

12.1. Glossaire, liste des versions/outils

12.2. Captures maquette (EVE-NG/GNS3), exports Terraform

12.3. Checklists (sécurité, déploiement, PRA)