Projet Collaboratif
CAS: SMART FACTORY

ELAN CONSULTING

SMARTFACTORY

SOMMAIRE

Introduction

I. Présentation de l’entreprise et reformulation du besoin

II. Contexte d’entreprise et contraintes

III. Proposition de la solution et architecture

IV. Coût total de la solution proposée

V. Mise en production

VI. Maintien en condition opérationnelle

VII. Stratégie de sauvegarde

Conclusion

ELAN CONSULTING

INTRODUCTION

Projet réalisé par **ELAN CONSULTING**, cabinet spécialisé dans la modernisation des systèmes d'information industriels

Mission : accompagner SMART FACTORY dans la refonte de son système d'information.

Objectifs : garantir la sécurité, l'agilité, la résilience et favoriser l'intégration d'une solution Cloud hybride

Solution proposée : une architecture mixte On-Premise + Cloud (Azure & OVH), adaptée au contexte multi-sites

Nathan



Chef de projet

Lucrèce



Expert cybersécurité

Avin



Ingénieur Système & Cloud

Euphrem



Ingénieur Réseau

I. Présentation de l’entreprise et Reformulation du Besoin



I. Présentation de l’entreprise et Reformulation du Besoin

Présentation de SMART FACTORY

- Groupe industriel fondé en 1980, spécialisé en équipements électroniques et électromécaniques.
- En pleine croissance, l’entreprise vise une transition vers l’Industrie 4.0

Besoins exprimés par la direction(19 Juin 2024)

- Moderniser une infrastructure IT vieillissante
- Automatiser les processus industriels
- Renforcer la cybersécurité (RGPD, protection SI)
- Favoriser la mobilité et la collaboration multi-sites
- Intégrer des solutions Cloud (Azure, OVH)
- Maîtriser les coûts à long terme

4 sites de production, 800 salariés :

- Strasbourg (siège) : R&D, Production, DG – 300 pers.
- Wolfisheim : Production & assemblage – 200 pers.
- Mittelhausbergen : Production robotisée – 150 pers.
- Lingolsheim : Production automatisée – 150 pers.

Contexte budgétaire :

- 6 M€ de budget global
- Estimations à prévoir sur :
  - Authentification / Messagerie / CRM
  - Hébergement / Stockage / Sauvegarde
  - Réseau / câblage / serveurs / périphériques

II. Contexte d’entreprise et contraintes

→ SWOT

→ Parties Prenantes

→ Topologie existante

→ Gestion des risques

→ Planification

II. Contexte d’entreprise et contraintes → SWOT

Forces (Strengths)

- Entreprise bien implantée sur 4 sites de production
- Volonté de modernisation
- Investissement significatif (6 M€).

Faiblesses (Weaknesses)

- Systèmes IT vieillissants et non virtualisée.
- Faible niveau de cybersécurité .
- Fragmentation des systèmes sur plusieurs sites.
- ERP maison obsolète.



Opportunités (Opportunities)

- Transition vers l’Industrie 4.0
- Solutions Cloud (hybride, souverain, public)
- Automatisation des chaînes de production
- Interconnexion via SD-WAN

Menaces (Threats)

- Risque de cyberattaques.
- Contraintes réglementaires (RGPD, NIS2)
- Coûts imprévus liés à la migration et aux mises à jour.
- Résistance interne au changement

II. Contexte d'entreprise et contraintes → Partie prenantes



Coté client – SMART FACTORY

Fonction	Rôle
Direction Générale	Prise de décision, et validation finale
Responsable IT	Supervision technique
Responsables des sites	Supervision Opérationnel
Comptabilité	Suivi budgétaire et validation des coûts
R & D	Suivi fonctionnel

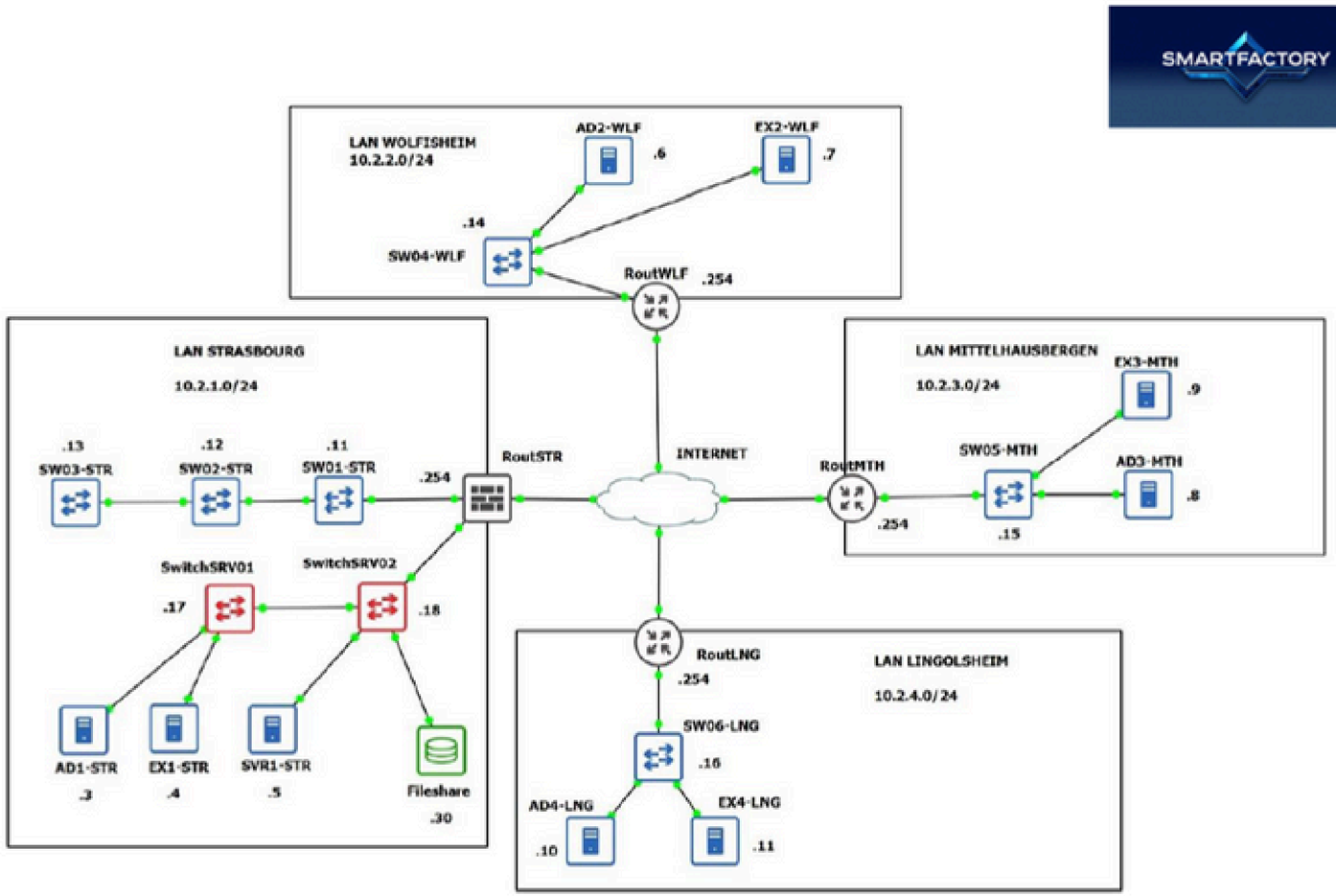
Coté Prestataire – ELAN CONSULTING

Consultant	Rôle
Nathan CRISPIN	Chef de projet – Coordination globale
Lucrèce SIGNING	Expert cybersécurité – Conformité, supervision, plan de remédiation
Avin MAAMO	Ingénieur Système – Virtualisation, serveurs, stockage
Euphrem Balounga	Ingénieur Cloud & Réseau – Architecture hybride, interconnexion

Côté fournisseurs – Prestataires externes

Fournisseur / Prestataire	Rôle / Contribution principale
Microsoft	Services cloud (authentification, messagerie, CRM, etc.)
OVH Cloud	Cloud souverain
Dell Technologies	Fournisseur des serveurs, postes de travail
Cisco	Équipements réseau (Switches, bornes Wi-Fi)
Stormshield	Pare-feu et sécurité réseau
Veeam	Solution de sauvegarde et PRA
Brother	Solutions d'impression
Alcatel	Téléphone ip

II. Contexte d’entreprise et contraintes → Topologie existante



Problèmes constatés :

Infrastructure non mutualisée entre les sites

Messagerie locale dépassée (Exchange 2010)

Absence de redondance et de haute disponibilité

Absence de supervision et de PRA

Stockage local sans sauvegarde cloud

II. Contexte d’entreprise et contraintes → Gestion des risques

a. Méthodologie AMDEC

Pour le projet SMART FACTORY, la méthode AMDEC (Analyse des Modes de Défaillance, de leurs Effets et de leur Criticité) a été retenue comme la plus adaptée.

Cette approche est particulièrement reconnue dans les environnements industriels, car elle permet d’anticiper les défaillances potentielles, d’en mesurer l’impact et de prioriser les actions de prévention.

Elle s’inscrit dans une logique proactive de maîtrise des risques, essentielle pour garantir la continuité de la production, la résilience de l’infrastructure IT et le respect des exigences de sécurité (RGPD, NIS2).



b. Analyse de Risques & Matrice

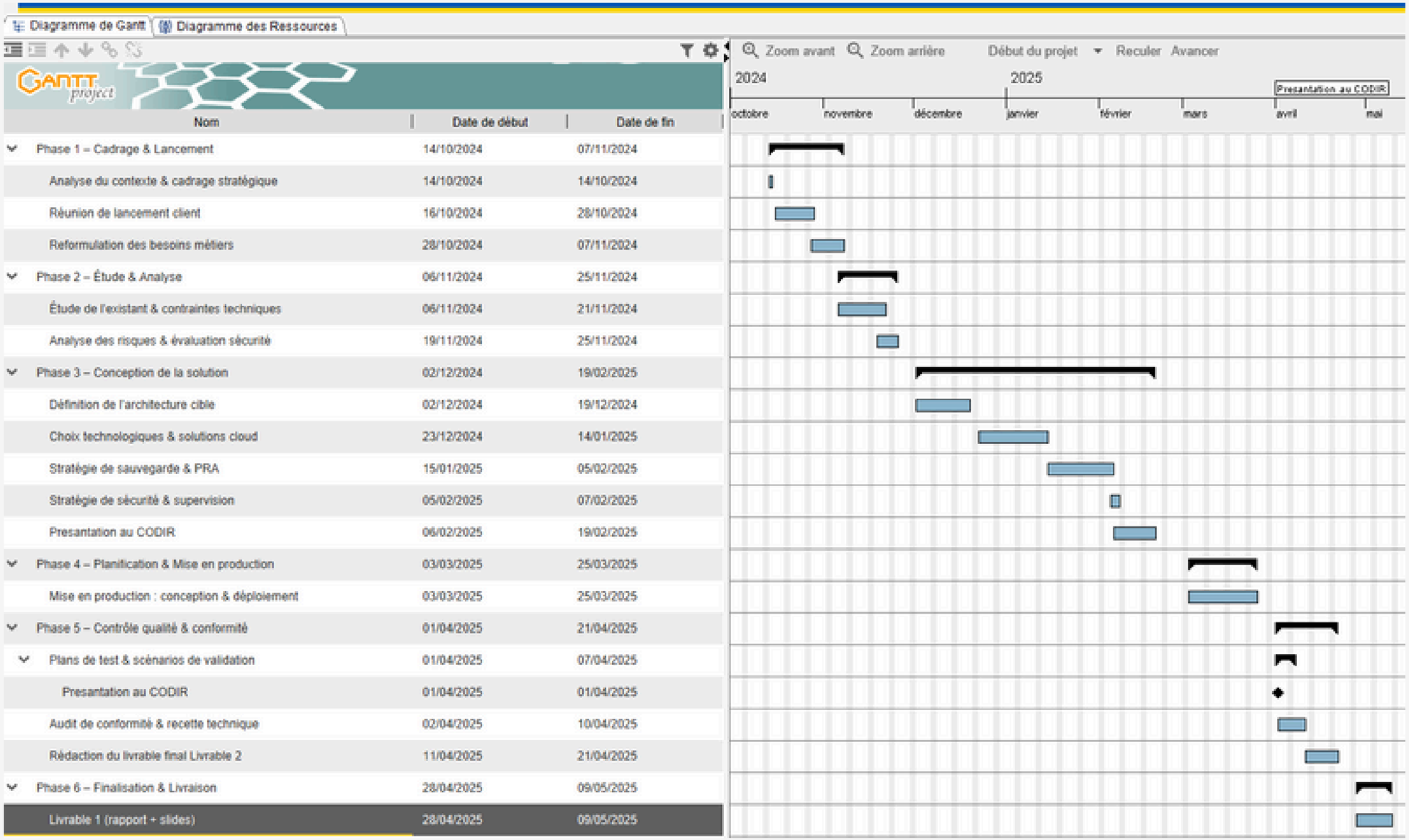
Excel matrice Analyse de risque.ods



c. SLA



II. Contexte d’entreprise et contraintes → Planification



Nom	Date de début	Date de fin
Phase 1 – Cadrage & Lancement	14/10/2024	07/11/2024
Analyse du contexte & cadrage stratégique	14/10/2024	14/10/2024
Réunion de lancement client	16/10/2024	28/10/2024
Reformulation des besoins métiers	28/10/2024	07/11/2024
Phase 2 – Étude & Analyse	06/11/2024	25/11/2024
Étude de l'existant & contraintes techniques	06/11/2024	21/11/2024
Analyse des risques & évaluation sécurité	19/11/2024	25/11/2024
Phase 3 – Conception de la solution	02/12/2024	19/02/2025
Définition de l'architecture cible	02/12/2024	19/12/2024
Choix technologiques & solutions cloud	23/12/2024	14/01/2025
Stratégie de sauvegarde & PRA	15/01/2025	05/02/2025
Stratégie de sécurité & supervision	05/02/2025	07/02/2025
Presantation au CODIR	06/02/2025	19/02/2025
Phase 4 – Planification & Mise en production	03/03/2025	25/03/2025
Mise en production : conception & déploiement	03/03/2025	25/03/2025
Phase 5 – Contrôle qualité & conformité	01/04/2025	21/04/2025
Plans de test & scénarios de validation	01/04/2025	07/04/2025
Presantation au CODIR	01/04/2025	01/04/2025
Audit de conformité & recette technique	02/04/2025	10/04/2025
Rédaction du livrable final Livrable 2	11/04/2025	21/04/2025
Phase 6 – Finalisation & Livraison	28/04/2025	09/05/2025
Livrable 1 (rapport + slides)	28/04/2025	09/05/2025

III. Proposition de la solution et architecture

→ Approche

→ Architecture

→ Industrie 4.0 / Azure IOT-HUB

→ VLAN

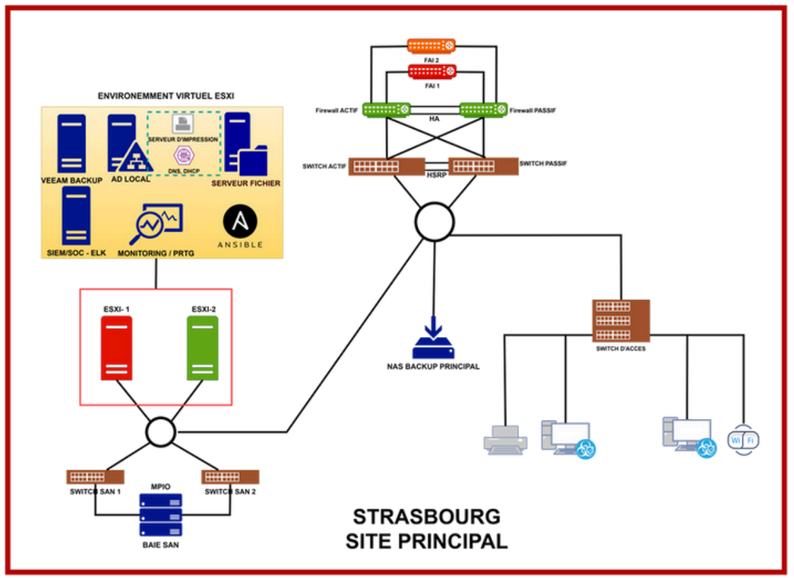
III. Proposition de la solution et architecture → Approche

L’approche choisie est hybride combinant :

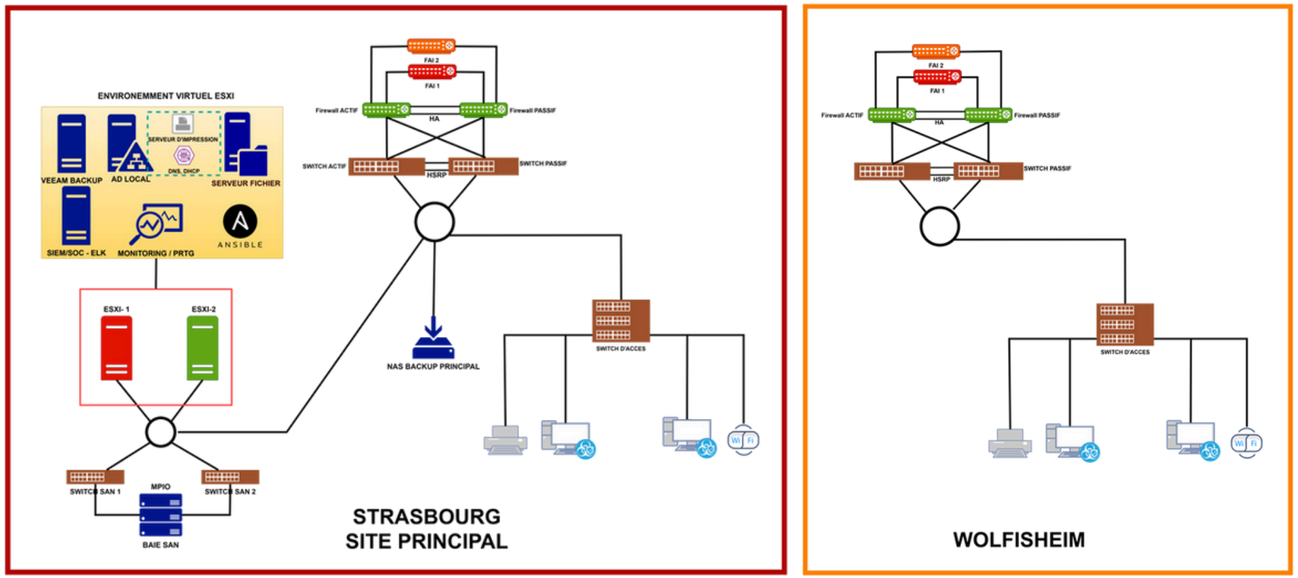
- Microsoft Azure
- OVH Cloud
- Une infrastructure On-premise

Cette stratégie combine les avantages du cloud public international (scalabilité, services avancés, performance) et ceux du cloud souverain français et européen (localisation, conformité RGPD, ANSSI, NIS2).

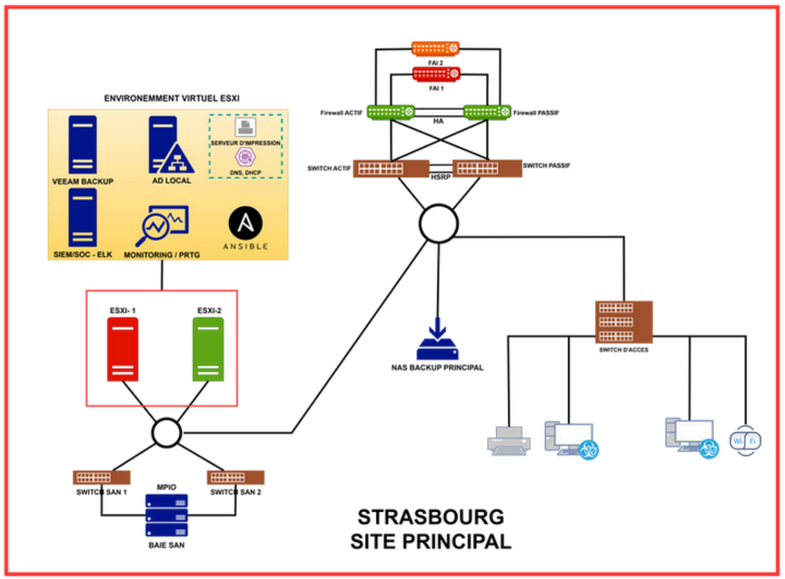
III. Proposition de la solution et architecture → Architecture

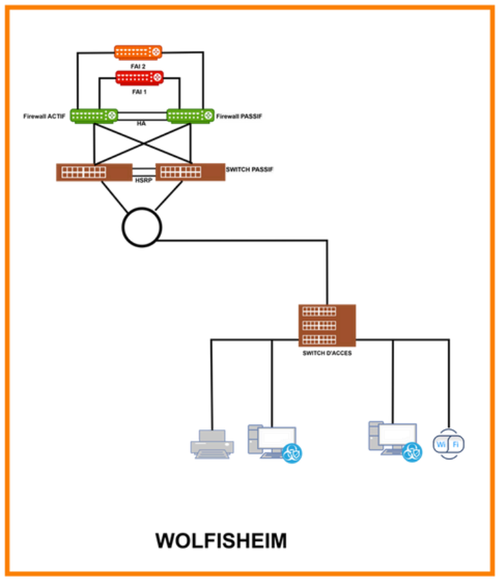


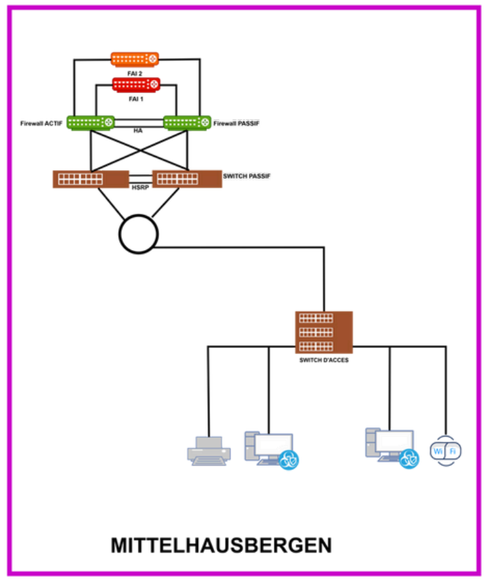
III. Proposition de la solution et architecture → Architecture



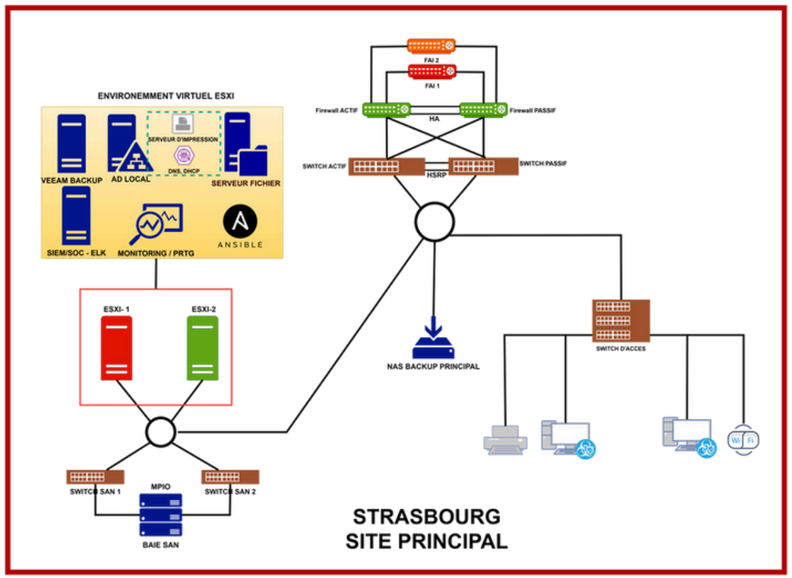
III. Proposition de la solution et architecture → Architecture

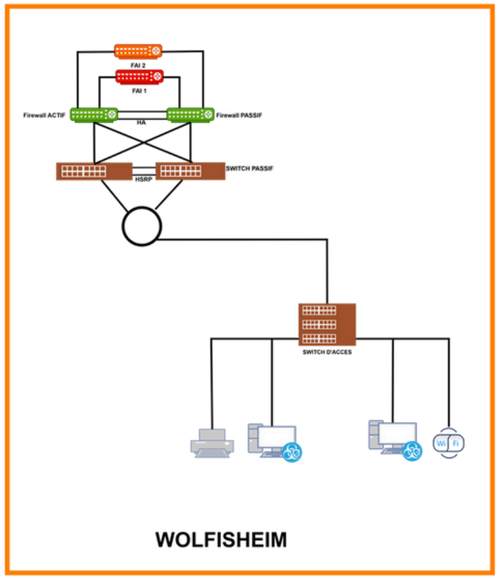


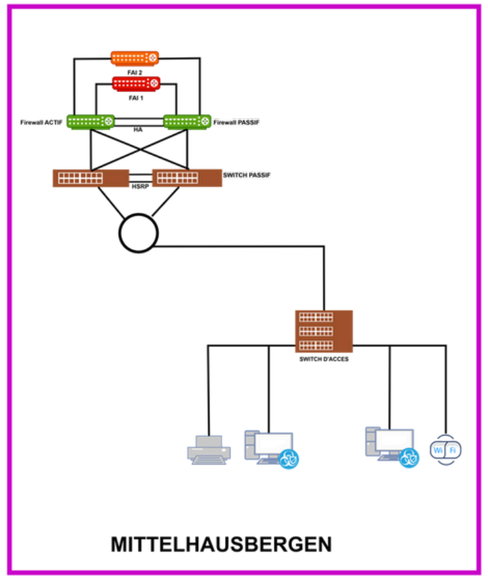


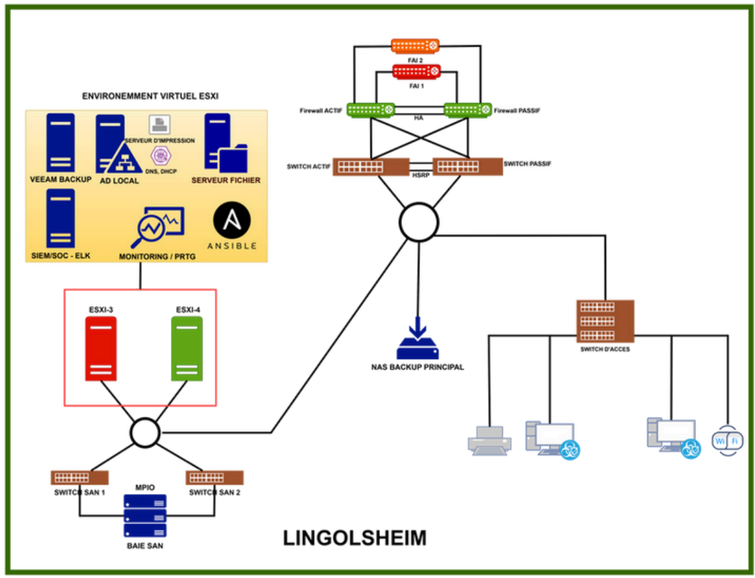


III. Proposition de la solution et architecture → Architecture

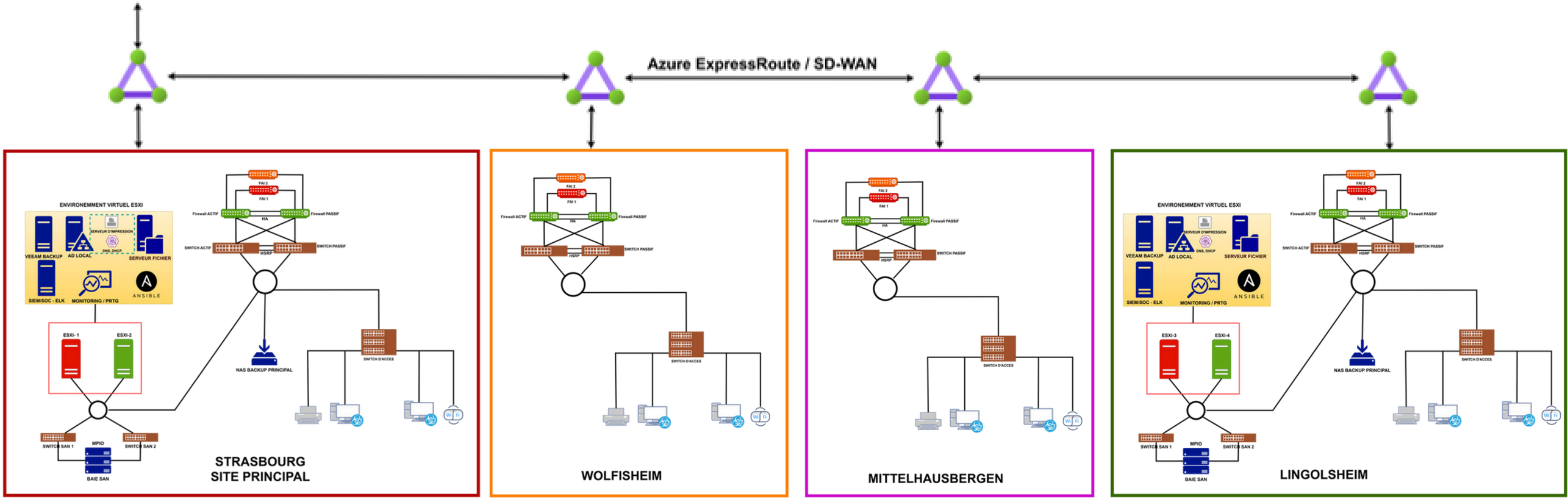




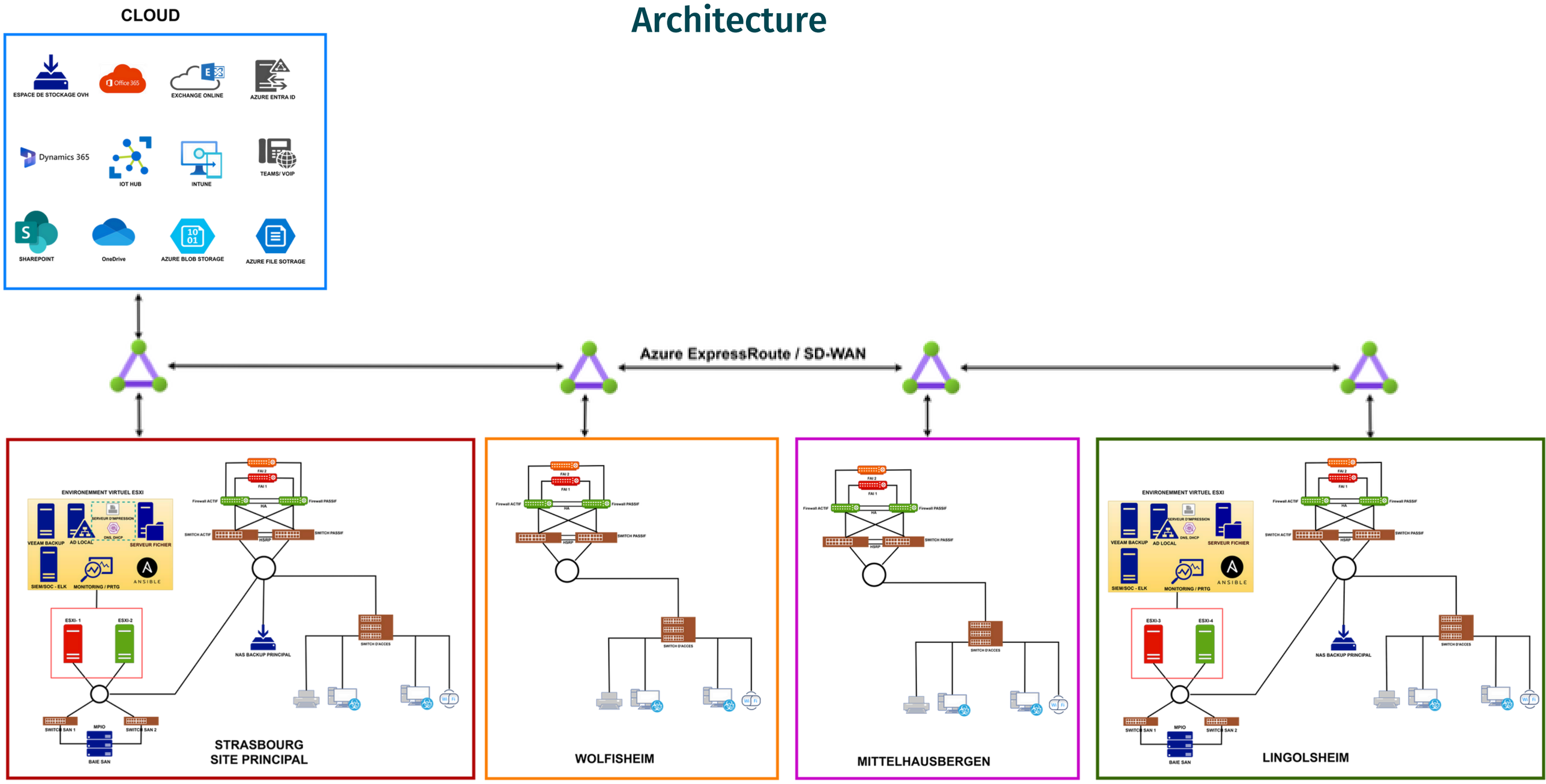




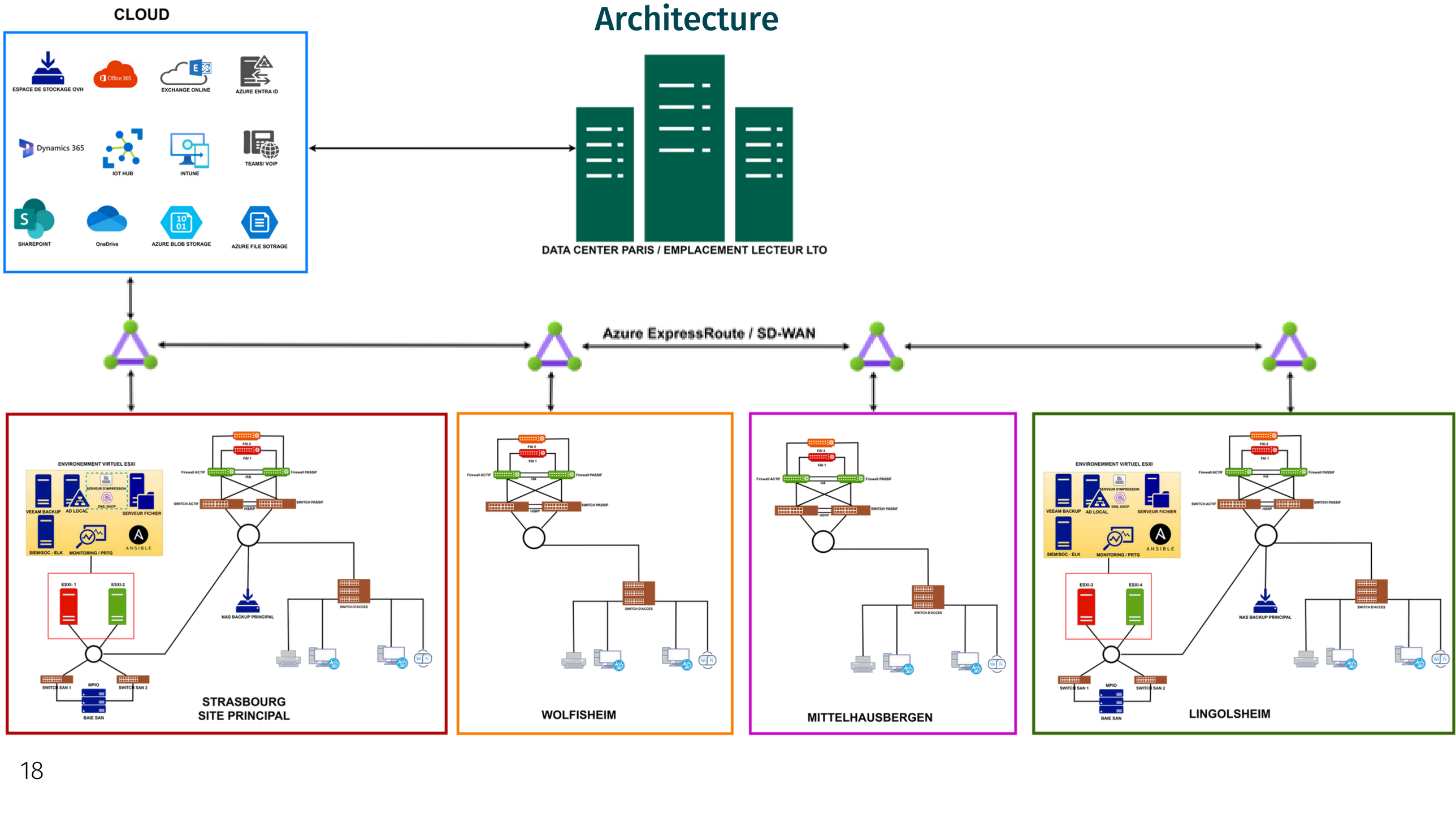
III. Proposition de la solution et architecture → Architecture



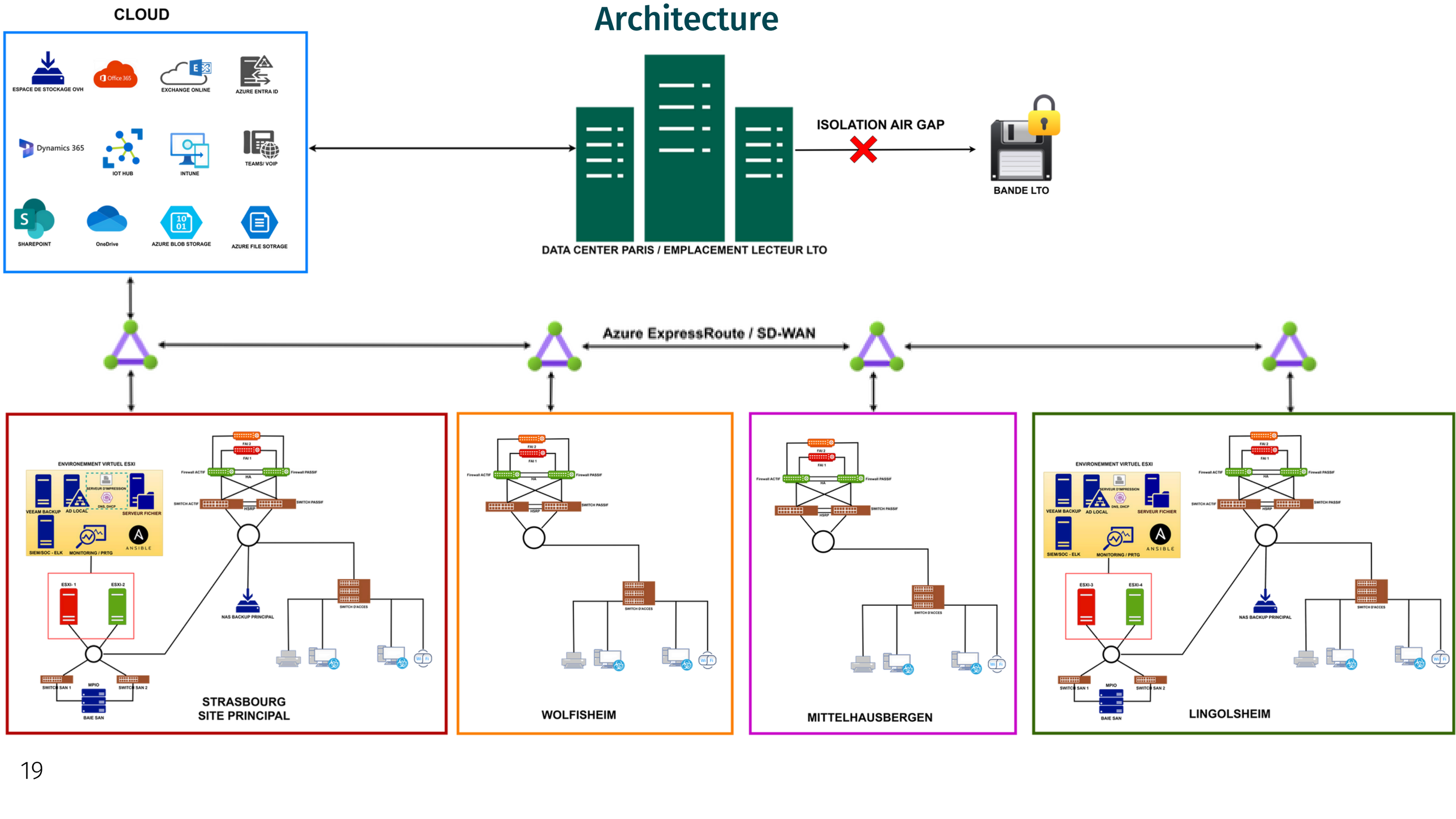
Architecture



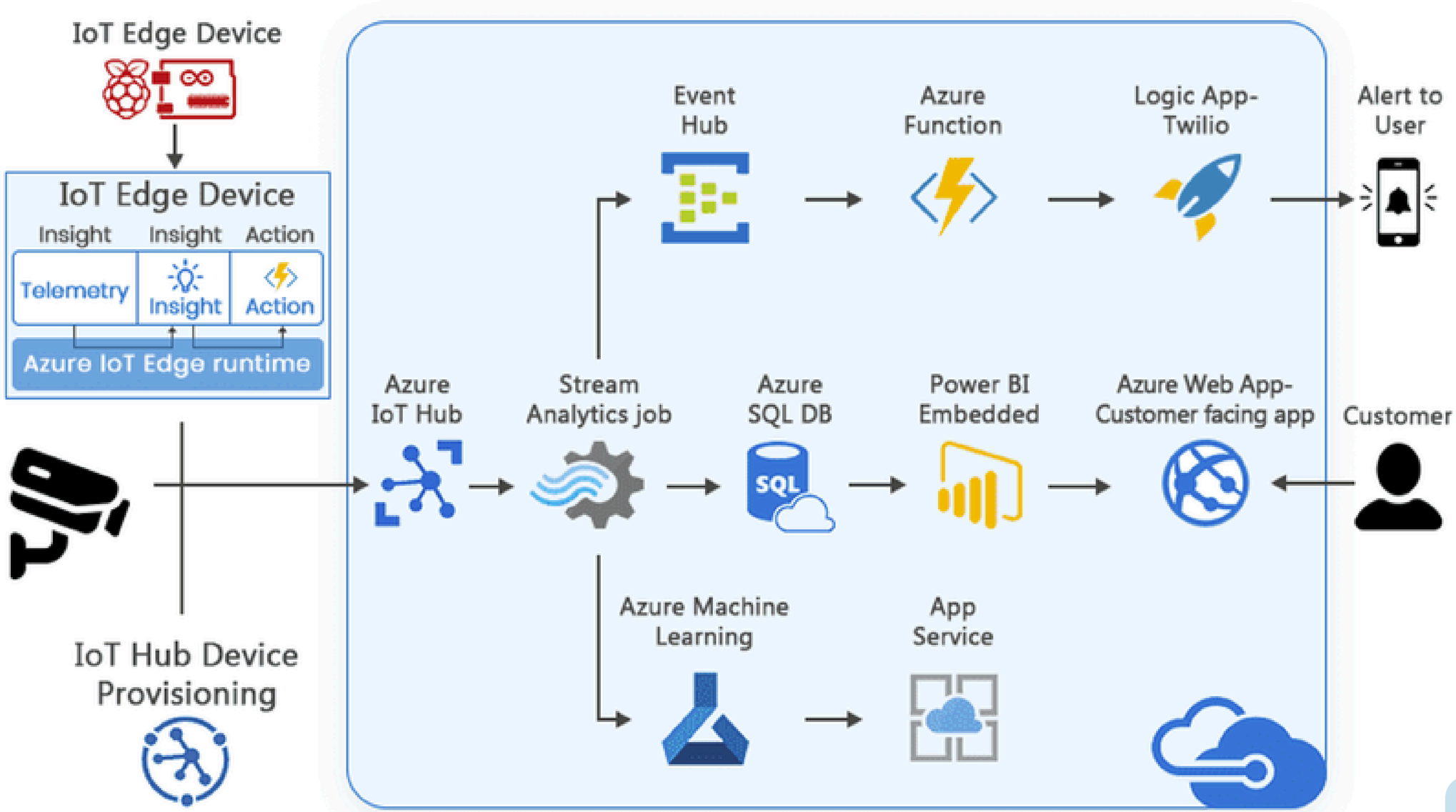
Architecture



Architecture



III. Proposition de la solution et architecture → Architecture Industrie 4.0 / Azure IOT-HUB



III. Proposition de la solution et architecture → VLAN

VLAN ID	Nom du VLAN	Usage
10	VLAN-Direction	Accès réservé à la direction générale
20	VLAN-Production	Machines de production, automates industriels
30	VLAN-IT	Serveurs, équipements IT, hyperviseurs ESXi
40	VLAN-Utilisateurs	Postes de travail
50	VLAN-Imprimantes	Imprimantes réseau
60	VLAN-Sauvegarde	NAS, Veeam Backup, stockage
70	VLAN-VoIP	Telephones IP, traffic voix dédié (avec QoS)
80	VLAN-WIFI-Interne	Wi-Fi sécurisé pour les employés (avec SSO)
90	VLAN-WIFI-Invités	Wi-Fi visiteurs, accès Internet uniquement
100	VLAN-MANAGEMENT	Gestion du réseau
110	VLAN-SUPERVSION	Surveillance du trafic réseau des services

IV. Couts total de la solution proposée

IV. Couts total de la solution proposée

Équipements	Quantité Total HT	Prix unitaire HT (€)	Total HT (€)
Serveurs principaux (Dell R660xs)	2	2966	5932
Serveur PRA (Dell R750)	1	4550	4550
Serveurs de virtualisation (Dell R750xs)	2	3640	7280
Serveur de fichiers	1	1 456	1456
NAS de sauvegarde	2	4 095	8190
SAN	2	1 090,99	2181,98
Switch SAN	4	345	1380
Switch Cisco Catalyst 9300	20	4200	84000
Firewall StormShield SN1100	8	6825	54600
Imprimantes	10	728	7280
Téléphone IP	180	260	46800
Onduleurs	2	910	1820
Borne WI-FI Cisco	40	430	17200
Licence Windows server	2	865	1730
VMware ESXI	2	1500	3000
Postes de travail (PC fixes)	800	850	680000
TOTAL			933 535,76 € HT

Solutions/Services	**Coût mensuel HT (€)**	**Coût annuel HT (€)**
Lecteurs de bandes LTO	4 935,78	4 935,78
Location baie 1 U pour lecteur LTO/ GLOBAL SP	150	1800
FAI (Orange)	3200	38400
FAI (Free)	2000	24000
Azure ExpressRoute	414	4968
SD-WAN (licences + abonnement opérateur)	800	9600
IOT hub/ Edition S1	29,744	356,928
Azure Files	149,55	1794,60
Azure Blob Storage	192	2304
NAS-HA OVH cloud	159	1908
Veeam Backup	240	2880
Azure Web App	605,90	7270,80
SIEM ELK	175	2100
GLPI ITSM	80	960
PRTG	508,25	6099
TOTAL		109377,108



IV. Couts total de la solution proposée



Budget prévisionnel pour 800 utilisateurs			
Description	Quantité	Coût mensuel HT (€)	Coût annuel HT (€)
Microsoft 365 Business standard	800	3,47 pour 1 utilisateur	33312
Microsoft Intune	800	2,30 pour 1 utilisateur	22080
Microsoft Entra ID P1	800	4,80 pour 1 utilisateur	46080
Dynamics 365	800	45,67 pour 1 utilisateur	438432
Salles Microsoft Teams Pro/VOIP	800	37,40 pour 1 utilisateur	359040
TOTAL			898944 € HT

Coûts globale

Catégorie	**Montant HT (€)**
Équipements réseau	933 535,76 €
Budget prévisionnel pour 800 utilisateurs	898944 €
Solutions/Services	109377,108
Coûts humains et d'installation	136372,35 €
Assistance et maintenance	23084,20 €
TOTAL GLOBAL	2101313.42 €

V. Mise en production

→ Application des strategies d’atténuation des risques

→ Phase de mise en production

Application des stratégies d’atténuation des risques

- Haute disponibilité & Continuité IT (PRA/PCA)
- Cybersécurité & RGPD
- Optimisation des coûts et des performances Cloud
- Déclenchement du PRA

Type d’incident	Plan d’action
Panne ERP & SQL	Bascule PRA sur Wolfisheim, restauration depuis une sauvegarde.
Cyberattaque majeure	Isolation des systèmes, récupération PRA, analyse forensique.
Défaillance réseau globale	Activation VPN de secours, failover SD-WAN.
Incident électrique prolongé	Basculer sur le site PRA Wolfisheim et Cloud Azure

Phase de Mise en production

Phase 1 – Conception et Préparation

Préparation

- Réception du matériel (serveurs, PC, réseaux…)
- Réservation des services cloud (Azure, OVH)

Validation de l’architecture cible

- Tests fonctionnels des principaux composants : AD, Azure Entra, M365, Dynamics
- Vérification de la connectivité intersites via SD-WAN

Sécurisation réseau

- Création de VLANs
- Configuration des pare-feux
- Mise en place de la QoS (priorité ERP et téléphonie)

Phase 2 – Migration technique

Migration des infrastructures IT

- Mise en place des VLANs
- Mise en service des pare-feux et du SIEM (ELK)
- Intégration des SD-WAN (connexion inter-sites)

Migration des services applicatifs

- ERP : migration total (Microsoft Azure).
- Migration ERP vers Microsoft Dynamics 365 sur Azure.
- Messagerie migrée vers Exchange Online avec synchronisation Active Directory hybride.

Migration des données et tests

- Données critiques migrées vers OVHcloud, copie locale sur NAS
- Tests de latence et validation des SLA
- Audit RGPD post-migration

Phase 3 - Déploiement final

Tests finaux

- Test de connectivité SD-WAN
- Vérification de la bascule automatique du PRA
- Tests de performance : temps de réponse ERP, CRM, mail

Sécurisation et monitoring

- Déploiement d’alertes automatiques
- Mise en place d’un support ITSM (GLPI)

Formation et Documentation

- Formation des équipes IT à la gestion des outils
- Rédaction de la documentation technique
- Rapport d’analyse de risques

VI. Maintien en condition opérationnelle

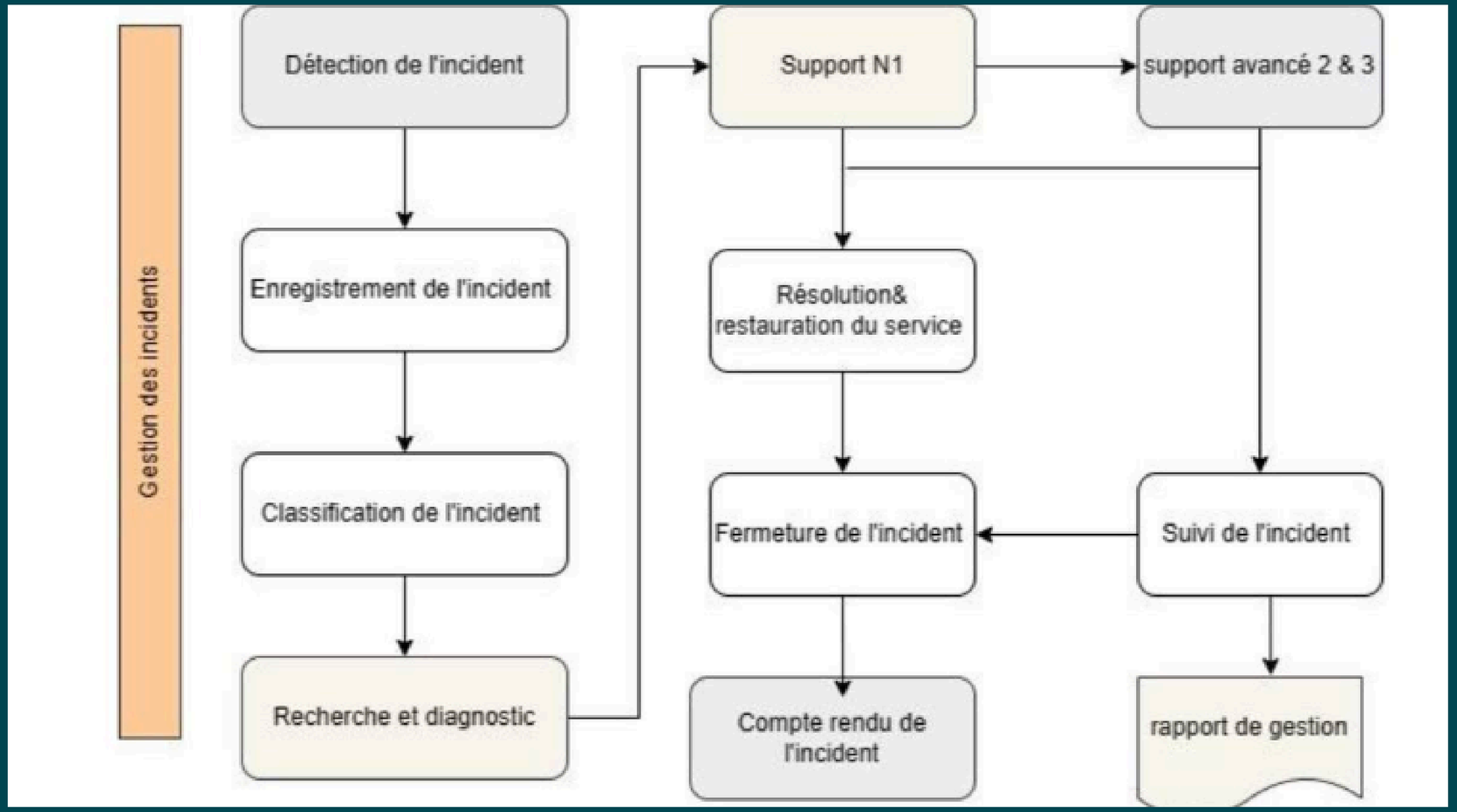
→ Gestion des incidents et des crises

→ Gestion des changements

Gestion des incidents et des crises

Un outil ITSM (GLPI)
est utilisé pour gérer les
demandes et les incidents.

Niveau	Responsabilités
Support N1	Assistance aux utilisateurs (accès, messagerie, CRM, etc.)
Support N2	Administration systèmes, réseau, virtualisation, sécurité
Support N3	Escalade fournisseurs (Azure, OVH), expertise cloud
Responsable MCO	Supervision globale, coordination, planification des évolutions



VI. Maintien en condition opérationnelle → Gestion des changements

Dans une logique d’exploitation continue, toute évolution majeure du système (mise à jour, correctif, ajout de fonctionnalités) doit être encadrée pour garantir la stabilité du SI.

Un processus simple est mis en place :

- Analyse préalable des risques
- Validation par la DSI
- Planification dans un créneau de déploiement contrôlé
- Vérification post-changement
- Mise à jour de la documentation

VII. Stratégie de Sauvegarde



VII. Stratégie de Sauvegarde

Nous adoptons la Stratégie 3-2-1-1-0 :

Principe	Mise en œuvre chez SMART FACTORY
3 copies	Données de production + NAS1 principal + NAS2 (secours)
2 supports	NAS (physique) + Cloud (OVH)
1 copie off-site	Backup encrypté hors site, stocké sur Blob Storage
1 copie offline	Sauvegarde sur bandes LTO (AirGap) déconnectées du réseau
0 erreur	Tests de restauration réguliers pour garantir l'intégrité des données

Supports de sauvegarde utilisés :

Support	Usage
NAS	Sauvegardes locales rapides (accès direct, court terme)
Bandes magnétique (LTO)	Pour une conservation à long terme et une protection contre les cybermenaces.
Stockage cloud (OVH, Azure)	Pour les copies hors site, en veillant à la conformité avec les réglementations (RGPD).

La fréquence de sauvegarde est adaptée à la criticité des données

Type de donnée	Fréquence	Exemples
Bases de donnes transactionnelles (ERP, CRM)	Quotidienne	En fin de journée (21h00)
Pour les fichiers moins sensibles (Documents métiers en production)	Hebdomadaire	Chaque dimanche à 23h00
Pour les archives et les données historiques (Archives, logs, historiques)	Mensuelle	1er de chaque mois (stockées 10 ans minimum)

Exigences - Normes Industrie 4.0

Tous nos fournisseurs cloud, répondent aux exigences de l’industrie 4.0 à travers et certifications suivantes :

- ISO 27001 : gestion de la sécurité de l'information.
- IEC 62443 : sécurité des systèmes industriels.
- ISO 9001 : gestion de la qualité.
- ISA-95 : intégration des systèmes industriels avec les systèmes informatiques.

CONCLUSION



Merci pour votre attention. L'équipe de ELAN CONSULTING s'engage à vous accompagner à chaque étape du projet pour assurer son succès et répondre à vos besoins. Nous restons à votre disposition pour toute question ou échange.