Situation 1 : Installation de 2 serveurs Windows 2025 AD DS, DNS, DHCP

Analyse du besoin :

Limite actuelle :

Actuellement, l'entreprise ne dispose pas d'ad (active directory). Les postes fonctionnent en session locale, ce qui pose problème, notamment en production où 12 employés se partagent 3 postes. L'absence de centralisation nuit à la gestion des utilisateurs, à la sécurité des données, et à l'efficacité globale de l'organisation.

L'objectif principal est **la mise en place d'un contrôleur de domaine Active Directory** pour centraliser l'authentification et la gestion des comptes utilisateurs.

Les besoins fonctionnels sont :

Active Directory :

- **Centraliser l'authentification :** Les utilisateurs doivent se connecter avec un seul identifiant et mot de passe sur tous les postes
- **Gérer les comptes utilisateurs :** Pouvoir créer, modifier, désactiver des comptes
- **Gérer les groupes :** Pouvoir créer des groupes de travail ou de services pour attribuer et faciliter la gestion des droits
- **Appliquer des politiques (GPO) :** Pouvoir imposer des règles à des utilisateurs ou groupes
- **Gérer les ordinateurs du domaine :** Ajouter des postes clients au domaine pour centraliser leur gestion
- **Sécuriser l'accès :** Assurer que seuls les utilisateurs autorisés peuvent accéder aux ressources

Juridique :

La solution envisagée implique la gestion de comptes utilisateurs et le stockage de fichiers, ce qui nécessite de prendre en compte plusieurs aspects juridiques :

- **Protection des données personnelles (RGPD)** : les informations liées aux utilisateurs (identifiants, activités, fichiers personnels) doivent être traitées conformément au Règlement Général sur la Protection des Données.
- **Sécurité des accès** : une politique de mot de passe robuste (longueur minimale, complexité, renouvellement régulier) doit être mise en place. Le chiffrement des données sensibles peut également être exigé pour garantir leur confidentialité, notamment lors des échanges sur le réseau.

La solution sera utilisée dans les locaux de l'entreprise, sur l'ensemble des postes connectés au réseau interne.
Elle impacte plusieurs processus métiers :

- La **gestion des utilisateurs** (création de comptes, attribution de droits)
- **L'accès aux documents partagés** au sein des services et en interne à l'entreprise
- La **sécurisation des postes** à travers des politiques définies

Les acteurs concernés sont :

- Les **employés** (utilisateurs finaux) qui bénéficieront d'une connexion simplifiée et d'un accès organisé aux fichiers
- Les **administrateurs** du système, chargés de la configuration, de la gestion et de la supervision de l'ensemble de la solution

Dossier de choix :

2 choix pour la solution possible :

- **AD local** : annuaire LDAP/Kerberos classique, gestion des utilisateurs, GPO (stratégies de groupe), contrôleurs de domaine sur site.
- **Azure AD** : service d'identité cloud orienté SSO pour applications web/SAAS, authentification moderne (OAuth/OIDC), intégration Office 365.

AD local		Azure AD	
Avantages	Défauts	Avantages	Défauts
Continuité hors-ligne : authentification/accès partages/imprimante même si la connexion internet est coupée	**Maintenance et compétences :** administration, mises à jour, sauvegardes à gérer en interne (ou externaliser)	**Haute disponibilité et redondance intégrée :** Microsoft assure la réplication sur plusieurs datacenters	**Coûts récurrents & licences :** nécessite une/des licence(s) => peu très vite augmenter et dépendant des tarifs de microsoft
Contrôle et souveraineté des données : données stockées en interne	**Scalabilité & mobilité :** pour accès SaaS/authentification depuis l'extérieur nécessite la configuration de solution complémentaires (VPN, Proxy…)	**Intégration native avec Office 365 / SaaS :** gestion centralisée des identités pour services cloud	**Dépendance à Internet :** connexion entreprise coupé => accès impacté
Gestion fine des postes Windows : gestion NTFS, GPO, scripts démarrage…	**Investissement initial :** investissement initial fort (server + licence) + temps d'administration/configuration	**Moins d'infrastructure physique à gérer :** pas de serveur en interne pour l'ad	
Coûts matériels prévisibles : pas d'abonnements cloud récurrents obligatoires		**Adapté aux utilisateurs en mobilité :** rend plus simple l'accès à l'ad depuis l'extérieur	
		Facturation flexible : modèle d'abonnement, coût suivant la charge	

Plusieurs points nous laissent tendre sur un **ad local** :

- L'accès aux ressources même en cas de coupure internet
- Le stockage des données en interne
- Une gestion plus fine des postes avec GPO et droit NTFS précis
- Coûts maîtrisés avec seulement un investissement initial
- Pas de besoin de mobilité dans l'entreprise car tous les postes sont fixes

Justification en termes de coût, de délai et de qualité

Critère	Justification
Coût	L'entreprise ne disposant pas de suffisamment de serveurs, il sera nécessaire d'acquérir une nouvelle machine physique et de créer une machine virtuelle afin d'héberger Windows Server 2025. Il faut donc prévoir un budget pour : - 1 serveurs (ou unités équivalentes) - 2 licences Windows Server 2025 Standard Ce coût reste maîtrisé au regard des bénéfices apportés (sécurité, organisation, continuité de service) et de l'absence de logiciels tiers payants
Délai	Le projet peut être déployé en **environ 5 jours ouvrés**, incluant l'installation, la configuration, les tests et la documentation
Qualité	La solution répond aux **besoins de centralisation, de sécurité et de résilience**, tout en restant **simple à administrer** pour l'équipe interne

Limites de responsabilité du prestataire

<u>Le prestataire est responsable :</u>

- De la mise en place conforme de la solution (serveurs, rôles, sécurité, documentation)
- De la formation minimale de l'équipe interne

Il ne peut être tenu responsable :

- De l'administration quotidienne si aucun contrat de maintenance n'est signé
- Des pertes liées à des pannes matérielles, erreurs humaines, ou défaut de sauvegarde en dehors de sa prestation
- De la gestion post-projet (sauvegarde, mise à jour, support technique)

Considérations éthiques et environnementales

- Les logiciels choisis respectent les **licences d'usage** et les **lois sur les données personnelles (RGPD)**
- Les GPO permettent d'**optimiser les consommations** (ex. : extinction automatique des postes, verrouillage automatique)

Évolution envisagée :

La solution repose sur la mise en place de **deux serveurs Windows Server** :

- Un **serveur (srv-ad01)**, avec comme rôle **AD DS**, **DNS** et **DHCP** : permet la centralisation des comptes et groupe utilisateurs, une meilleure sécurité avec la mise en place d'autorisation et de règles via GPO : Nécessite l'achat d'un nouveau serveur
- Un **Windows serveur virtuel (vm-ad02) sur le srv-prox01**, avec comme rôle la **réplication AD**, un **DHCP en mode load balancing**, **redondance DNS** : permet d'avoir une tolérance de panne si le ad01 vient à avoir un problème, le ad02 prendra relais pour l'AD et le DHCP.
- **Pourquoi ne pas utiliser qu'un seul serveur ?** Tout centraliser sur un seul serveur créerait un point unique de défaillance : si **ad01** tombe, tous les services (authentification, DNS, DHCP, etc.) deviendraient inaccessibles.
  C'est pourquoi une architecture avec deux contrôleurs de domaine est mise en place. Le ad01 joue le rôle principal, tandis que le **ad02** assure la redondance des services critiques (Active Directory, DNS).

Spécifications techniques

Élément	Détail
Système d'exploitation	Windows Server 2025 Standard (x2 licences)
AD DS	Domaine unique, réplication entre ad01 et ad02
DNS	Rôle intégrée à l'AD
DHCP	Configuration en mode **load balancing** entre ad01 (principal) et ad02 (secondaire), pour assurer la continuité de l'attribution IP
Sécurité	Politique de mot de passe forte, audit des connexions, droits NTFS + partages précis

Composants impactés de l'architecture technique :

Les principaux composants touchés par cette évolution sont :

- **Postes de travail :** Ils devront être intégrés au domaine Active Directory. Leurs modes de connexion seront modifiés (compte local → compte domaine). Ils reçoivent leur configuration réseau automatiquement (IP, passerelle…) depuis le serveur AD.
- **Comptes utilisateurs :** Gestion centralisée via l'AD au lieu de la création locale. La création/suppression/modification devient plus rigoureuse.
- **Infrastructure réseau (switch, câblage, DHCP, DNS) :** Un minimum de configuration réseau est nécessaire pour garantir la communication entre les serveurs et les postes. L'AD nécessite notamment un service DNS fonctionnel. Le serveur AD devient aussi serveur DHCP. Il prend le rôle de distribution des adresses IP, ce qui simplifie la gestion réseau et évite les IP statiques ou mal configurées.
- **Authentification :** Les postes et utilisateurs doivent passer par le serveur AD pour valider leurs identifiants.
- **Sécurité et gestion des droits :** Mise en place de stratégies de groupe (GPO) appliquées aux utilisateurs et ordinateurs pour uniformiser la configuration, renforcer la sécurité et limiter les actions non autorisées.

Risques liés à une mauvaise utilisation ou à un dysfonctionnement

Mauvaise utilisation :

- **Mauvaises pratiques de mot de passe** : si les politiques ne sont pas bien configurées, des mots de passe faibles peuvent mettre en danger le domaine
- **Partages mal configurés** : une mauvaise attribution des droits peut rendre des fichiers sensibles accessibles à tous ou inaccessible aux utilisateurs en ayant besoin.
- **Ajout non maîtrisé de machines au domaine** : sans supervision, cela peut entraîner des erreurs ou des failles de sécurité.

Dysfonctionnement technique :

- **Panne du serveur AD principal** : sans redondance, plus aucune authentification n'est possible. D'où l'intérêt du serveur secondaire. Cela impact également le service DHCP, les postes ne reçoivent plus d'adresse IP, ils perdent donc la connexion réseau (et donc le domaine, le partage de fichiers…).
- **Mauvaise configuration du DHCP :** Si le serveur donne une mauvaise IP ou un DNS externe, les postes peuvent ne plus joindre le domaine.
- **Problèmes de DNS** : si le DNS lié à l'AD est mal configuré ou en panne, les postes ne peuvent plus contacter le domaine. Rendant impossible la connexion pour un utilisateur ne s'étant jamais connecté à un poste avant, un arrêt des applications des GPO, une perte d'accès aux ressources (telle que le partage de fichier) ...
- **GPO mal appliquées** : une mauvaise stratégie peut bloquer l'accès aux ressources essentielles ou provoquer des dysfonctionnements utilisateurs.

Éléments à sauvegarder :

Pour garantir la **continuité de service** en cas d'incident, les sauvegardes doivent couvrir :

- La **base Active Directory** (AD DS) : essentielle pour l'authentification et la gestion des utilisateurs

Journalisation :

Permet d'assurer la **traçabilité des transactions et des accès** :

- **Connexions** (authentifications réussies/échouées)
- **Accès aux fichiers** (écriture, suppression)

Procédures d'alerte associées au service

Pour permettre une **réaction rapide en cas de problème**, les alertes doivent être mises en place sur les services critiques :

- **Surveillance via Zabbix**
- Déclenchement d'une alerte en cas de :
    - Échec d'authentification répété (tentative d'intrusion)
    - Espace disque faible sur les serveurs
    - Échec de la réplication AD
    - Panne d'un service (DHCP, DNS, partage réseau)

Solutions de fonctionnement en mode dégradé et procédures de reprise

Mode dégradé :

Prévu pour assurer une **tolérance aux pannes** :

- **Redondance Active Directory** : le ad02 prend le relais en cas de panne du ad01
- **DHCP en mode load balancing** : permet l'attribution IP même si un serveur est inactif

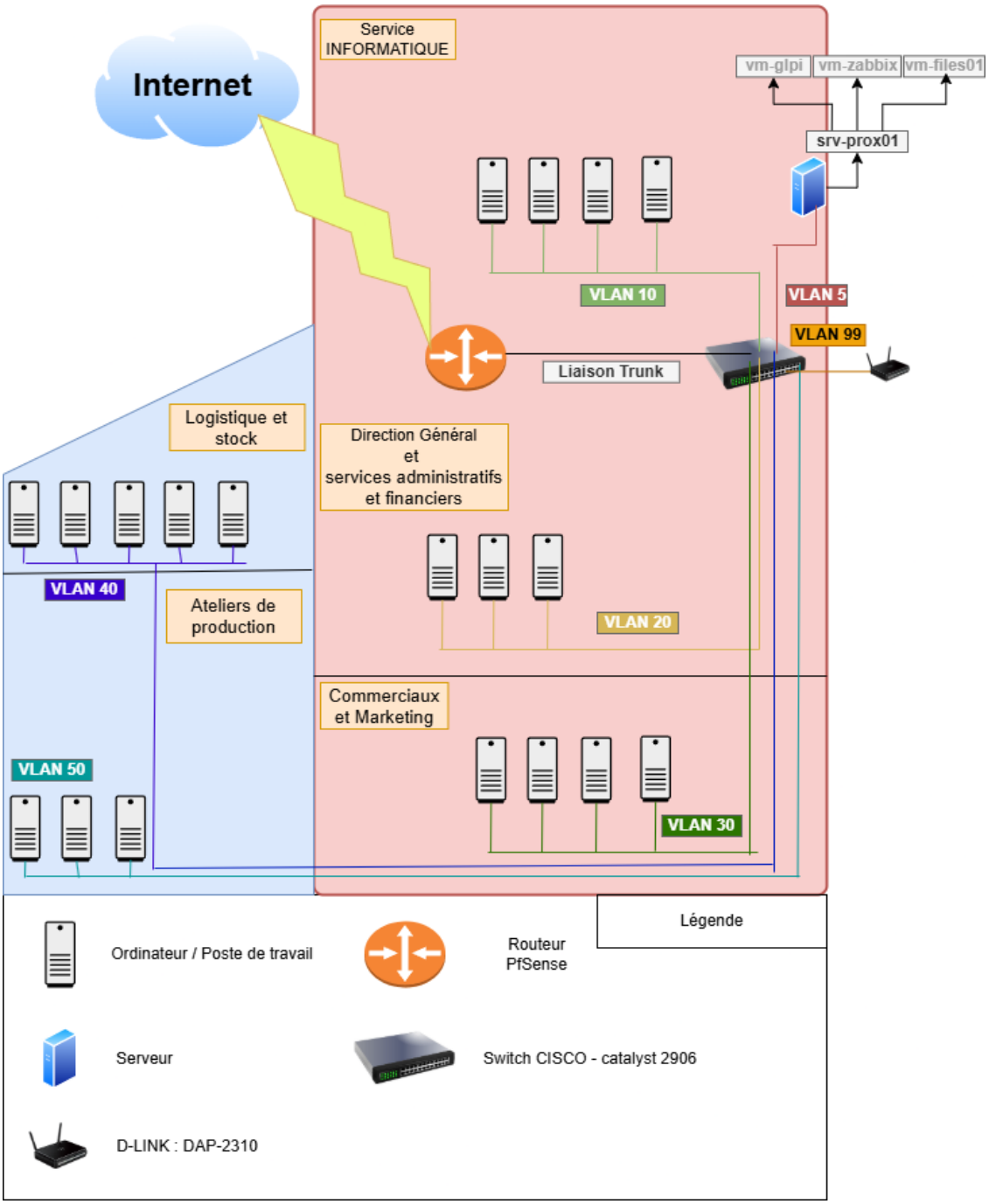
Reprise du service :

En cas d'interruption totale ou partielle, **redémarrage séquencé des services** (AD → DNS → DHCP)

Maquette fonctionnelle :

La maquette représente l'infrastructure actuelle de l'entreprise et l'intégration des deux windows serveur (un physique et une machine virtuel).

Schéma final :



Machine	IP	Masque	VLAN
srv-prox01	192.168.5.2	255.255.255.0	5
vm-glpi	192.168.5.3	255.255.255.0	5
vm-files01	192.168.5.4	255.255.255.0	5
vm-zabbix	192.168.5.10	255.255.255.0	5
srv-ad01	192.168.5.5	255.255.255.0	5
vm-ad02	192.168.5.6	255.255.255.0	5

Tests d’acceptation à réaliser

Active Directory (AD DS)

- Test de création/modification/suppression d’un utilisateur ou groupe
- Test de connexion d’un utilisateur à un poste du domaine
- Test d’application d’une GPO
- Test de réplication AD entre ad01 et ad02

DNS / DHCP

- Test de résolution de noms
- Test d’attribution IP dynamique via DHCP
- Test du mode **load balancing** DHCP

Droit d’accès serveur de fichiers

- Test d’accès aux dossiers partagés selon les droits NTFS définis
- Test de lecture/écriture/suppression par un utilisateur autorisé
- Test du refus d’accès pour un utilisateur non autorisé
- Test de logs d’accès aux fichiers (journalisation)

Redondance et continuité

- Test de la disponibilité des services si **ad01 est arrêté** (authentification, DHCP, DNS)

Redémarrage des serveurs pour vérifier le redémarrage automatique des rôles