TP Architecture Azure

Table des matières

I. Présentation du Projet

Ce document présente la conception détaillée de l'architecture cloud pour le projet InnovTech, entièrement déployée sur la plateforme Microsoft Azure. L'objectif principal est de garantir un environnement performant, évolutif, et surtout, sécurisé, en s'alignant sur les meilleures pratiques de gouvernance Azure.

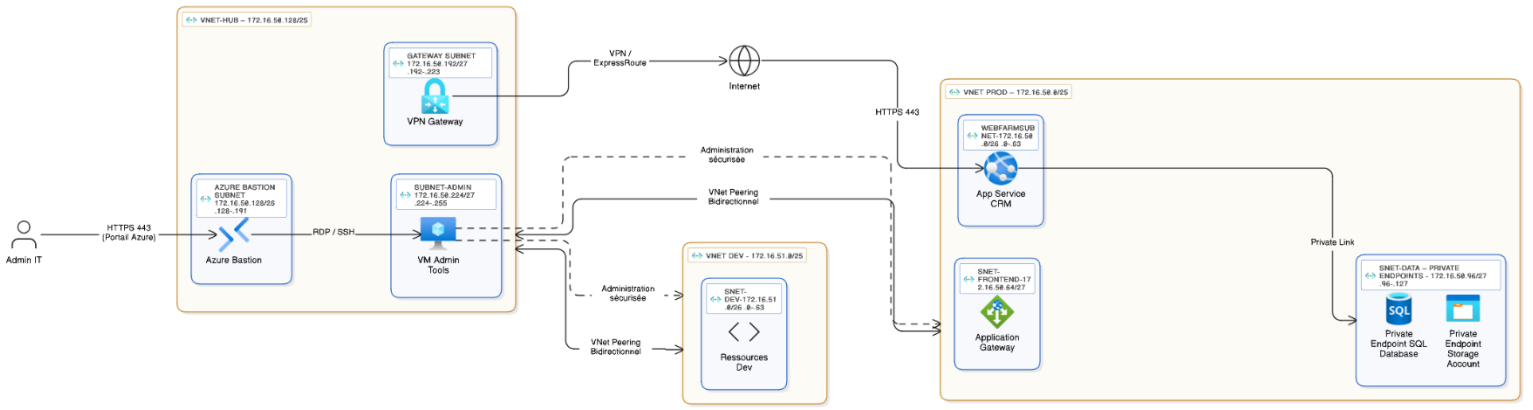
L'architecture repose sur le modèle éprouvé Hub-and-Spoke , qui permet une isolation stricte entre les environnements de Production (Prod) et de Développement (Dev) tout en centralisant les services de gestion et de sécurité au sein du Hub.

Le défi initial a été de planifier l'adressage IP à partir d'un espace unique de 172.16.50.0/23 (soit 512 adresses hôtes au total) afin de bâtir un socle réseau robuste.

Objectifs Clés de la Conception :

- Concevoir une architecture complète basée sur le modèle Hub-and-Spoke.
- Effectuer le calcul exhaustif de l'adressage IP en tenant compte des 5 adresses IP réservées par Azure.
- Mettre en œuvre les bonnes pratiques Azure : PaaS, Zero Trust, RBAC, et Azure Policy.
- Établir une estimation budgétaire réaliste.
- Fournir un plan de déploiement clair et structuré (Build Plan).

II. Schéma et Structure Réseau



eraser

L'architecture illustre l'utilisation du modèle Hub-and-Spoke pour une gestion de réseau et une posture de sécurité centralisées.

Structure des VNets et Relations :

VNet	Type	CIDR	Plage d'adresses	Peering
VNet-Hub	Hub	172.16.50.128/25	172.16.50.128 172.16.50.255	Bidirectionnel vers VNet-Prod et VNet-Dev
VNet-Prod	Spoke	172.16.50.0/25	172.16.50.0$ 172.16.50.127	Bidirectionnel avec VNet-Hub
VNet-Dev	Spoke	172.16.51.0/25	172.16.51.0 172.16.51.127	Bidirectionnel avec VNet-Hub
VNet-Libre	Réservé	172.16.51.128/25	172.16.51.128 172.16.51.255	Aucun (Réserve future)

Composants Clés par Zone (VNet)

Zone	Composants clés présents	Accès Bastion obligatoire
VNet-Hub	Azure Bastion, VPN Gateway (future), VMs Outils Admin.	Oui. Bastion est déployé dans son propre subnet (*AzureBastionSubnet*).
VNet-Prod	App Service, Azure SQL DB (via Private Endpoint), Key Vault (via Private Endpoint), Storage Account (via Private Endpoint).	Oui. Accès aux VMs, si présentes, pour maintenance via Bastion.
VNet-Dev	App Service de Dev, Azure SQL DB de Dev, Key Vault de Dev.	Oui. Accès aux environnements de test et debug via Bastion.

III. Planification d'Adressage Complet

L'espace initial 172.16.50.0/23 (512 adresses) est subdivisé en 4 VNets de 128 adresses chacun, en utilisant le masque /25.

1. Tableau d’adressage des VNets

VNet	CIDR	Plage d'adresses	Total Adresses	Utilisables (Total - 5)	Justification technique
VNet-Prod	172.16.50.0/25	172.16.50.0-172.16.50.127	128	123	Espace dédié à la Production, supportant des subnets /26 pour l'intégration App Service.
VNet-Hub	172.16.50.128/25	172.16.50.128-172.16.50.255	128	123	Centralisation des services d'infrastructure (Bastion, Gateway, Outils Admin).
VNet-Dev	$172.16.51.0/25	172.16.51.0 - 172.16.51.127	128	123	Assure l'isolation de l'environnement de Développement.
VNet-Libre	$172.16.51.128/25	172.16.51.128-172.16.51.255	128	123	Réserve pour future extension (ex : Staging ou DMZ).

2. Calcul des Sous-réseaux (Subnets)

Sous-réseaux du VNet-Hub (172.16.50.128/25)

Sous-réseau	CIDR	Plage d'adresses	Total Adresses	Utilisable (Total - 5)	Justification technique du choix
AzureBastionSubnet	172.16.50.128/26	172.16.50.128-172.16.50.191	64	59	Masque /26 choisi comme **bonne pratique Azure** pour l'évolutivité du service Bastion (minimum requis : /27).
GatewaySubnet	172.16.50.192/27	172.16.50.192-172.16.50.223	32	27	Masque /27 recommandé pou une Gateway VPN/ExpressRout robuste (minimum requis : /29).
ManagementSubnet	172.16.50.224/27	172.16.50.224-172.16.50.255	32	27	Pour les *Jumpboxes* (VMs Outils Admin) uniquement accessibles via Bastion.

Sous-réseaux du VNet-Prod (172.16.50.0/25)

Sous-réseau	**CIDR**	**Plage d'adresses**	**Total Adresses**	**Utilisable (Total - 5)**	**Justification technique du choix**
WebFarmSubnet	172.16.50.0/26	172.16.50.0-172.16.50.63	64	59	Taille idéale pour l'intégration VNet régionale de l'App Service, supportant son *scale-out* (jusqu'à 64 instances).
FrontendSubnet	172.16.50.64/27	172.16.50.64-172.16.50.95	32	27	Sous-réseau pour les services frontaux tels qu'*Application Gateway* ou *Load Balancer*.
DataSubnet	172.16.50.96/27	172.16.50.96-172.16.50.127	32	27	**Private Link Subnet** : Sous-réseau dédié à l'hébergement des **Private Endpoints** (SQL DB, Key Vault, Storage).

Sous-réseaux du VNet-Dev (172.16.51.0/25)

Sous-réseau	CIDR	Plage d'adresses	Total Adresses	Utilisable (Total - 5)	Justification technique du choix
Simplicite1Subnet	172.16.51.0/26	172.16.51.0-172.16.51.63	64	59	Subnet d'intégration VNet pour l'App Service de Développement.
Simplicite2Subnet	172.16.51.64/26	172.16.51.64-172.16.51.127	64	59	Subnet de réserve pour les *Private Endpoints* de Dev ou une seconde application isolée.

IV. Identités, Groupes et Contrôle d'Accès

La gestion des identités s'appuie sur Azure AD (Entra ID) et le contrôle d'accès est régi par le RBAC (Role-Based Access Control) selon le principe du moindre privilège, renforcé par PIM et MFA.

Catégories d'Utilisateurs :

- Admins IT : Gestion complète et haut niveau de l'infrastructure Azure.
- Développeurs : Déploiement d'applications, consultation des logs et gestion de l'environnement de développement.
- Auditeurs : Rôle de consultation (Lecture Seule) des configurations et des logs de sécurité.

Groupes Azure AD

Nom du Groupe Azure AD	Rôles Assignés (RBAC)	Portée
InnovTech-IT-Admins	Contributeur (*Contributor*)	Abonnement (*Subscription*) (via PIM)
InnovTech-Dev-Ops	Contributeur de Site Web (*Website Contributor*)	Groupe de Ressources (Prod/Dev)
InnovTech-Auditors	Lecteur (*Reader*)	Abonnement (*Subscription*)
InnovTech-Logs-Readers	Lecteur de Logs (*Logs Reader*)	Ressource (*Log Analytics Workspace*)

Permissions Détaillées (RBAC)

Tâche	Groupe / Entité Responsable	Rôle RBAC	Portée	Justification et Point Clé
Administration des ressources	**InnovTech-IT-Admins**	Contributeur (*Contributor*)	Niveau **Subscription**	Rôle soumis à **PIM** et nécessitant la **MFA** pour l'activation JIT.
Déploiement d'application	**InnovTech-Dev-Ops**	Contributeur de Site Web (*Website Contributor*)	**Resource Group** (spécifique Prod/Dev)	Ce rôle est suffisant pour le déploiement du code et la configuration des slots sans modification du réseau.
Lecture des logs	**InnovTech-Auditors** et **InnovTech-Logs-Readers**	Lecteur ou Lecteur de Logs	**Subscription** (Auditeurs) ou **Ressource** (Logs Readers)	Vue en Lecture Seule pour l'audit et le *troubleshooting* quotidien.
Accès au Key Vault (secrets)	**Identité Managée** de l'App Service	*Key Vault Secret User* ou permission *Get*	**Ressource** (Key Vault spécifique)	L'accès est accordé à l'application et non à un utilisateur humain, via le *Private Endpoint*.

V. Architecture Applicative et Données

L'architecture est spécifiquement optimisée pour le PaaS afin de minimiser les frais opérationnels.

- **App Service (Plan et Scale-out)**
    - **Plan :** Premium V3 (P1v3 minimum), car ce niveau est obligatoire pour l'Intégration VNet Régionale.
    - **Scale-out :** Utilisation de l'Autoscale basé sur l'utilisation du CPU (ex : montée à 70%, descente à 30%) pour une élasticité optimale.
    - **Intégration VNet :** La VNet Integration Régionale est utilisée pour connecter l'App Service au WebFarmSubnet (), assurant que le trafic sortant vers les services de données reste privé.
- **Azure SQL Database**
    - **Accès :** Exclusivement privé via un Private Endpoint déployé dans le DataSubnet de VNet-Prod. L'accès public est désactivé.
    - **Sécurité :** L'authentification Azure AD est utilisée (Identité Managée pour l'App Service).
- **Key Vault (Protection des Secrets)**
    - **Contenu :** Stockage des chaînes de connexion SQL et des certificats.
    - **Accès :** Sécurisé via un Private Endpoint dans le DataSubnet. Seules les Identités Managées de l'App Service ont les permissions d'accès aux secrets.
- **Storage Account (5 To)**
    - **Accès :** Sécurisé via un Private Endpoint dans le DataSubnet.
    - **Gestion du Cycle de Vie (*Lifecycle Management*) :** Politique mise en place pour réduire les coûts :
        - Déplacement des données vers le niveau **Cool** après 30 jours.
        - Déplacement des données vers le niveau **Archive** après 90 jours.
        - Suppression automatique après 365 jours.

VI. Architecture de Sécurité (Zero Trust)

La sécurité est intégrée de manière proactive à chaque couche, en adhérant au modèle *Zero Trust* : Ne jamais faire confiance, toujours vérifier.

- **Azure Policy (Gouvernance)**
  - **Allowed Locations :** Limite le déploiement à France Central.
  - **Deny Public IP :** Interdit l'association d'adresses IP publiques sur les interfaces réseau, empêchant l'exposition accidentelle.
- **Accès Zero Trust : Bastion**
  - L'accès RDP/SSH aux éventuelles VMs est uniquement autorisé via Azure Bastion (dans VNet-Hub), éliminant l'ouverture de ports d'administration sur Internet.
- **Isolation des Données (Private Link)**
  - Tous les services critiques (SQL DB, Key Vault, Storage Account) sont accédés via Private Endpoints (*Private Link*) depuis le DataSubnet, maintenant le trafic sur le réseau privé d'Azure.
- **Groupes de Sécurité Réseau (NSG)**
  - **NSG sur WebFarmSubnet :** Autorise le trafic web entrant et le trafic sortant vers le DataSubnet (connexion à SQL/KV/Storage).
  - **NSG sur DataSubnet :** Restreint le trafic entrant exclusivement au WebFarmSubnet et au ManagementSubnet.
- **MFA + PIM**
  - L'authentification Multi-Facteurs (MFA) est obligatoire pour tous les accès Azure.
  - Le Privileged Identity Management (PIM) impose une activation Juste-À-Temps (JIT) et limitée dans le temps pour les rôles à haut privilège (Contributeur).
- **Surveillance Azure Monitor et Alerting**
  - Les métriques sont centralisées dans un Log Analytics Workspace.
  - Une règle d'Alerte est configurée sur l'App Service pour notifier l'équipe si l'utilisation CPU dépasse **80%** pendant 5 minutes.

VII. Plan de Déploiement Azure (Build Plan)

Le déploiement est organisé en phases séquentielles.

Phase 1 : Gouvernance

Ressources déployées	**Ordre logique**	**Points d'attention techniques**
Management Groups, Abonnement, Groupes AD	1. Définition de la hiérarchie et création des Groupes AD.	S'assurer des droits d'administration au niveau du Root MG.
Azure Policy	3. Déploiement des Policies *Allowed Locations* et *Deny Public IP*.	Déploiement initial en mode *Audit* pour validation.
PIM et MFA	4. Configuration de PIM sur les rôles Contributeur.	Tester le processus d'élévation de privilège via PIM.

Phase 2 : Réseau

Ressources déployées	**Ordre logique**	**Points d'attention techniques**
VNets et Subnets	1. Création des 3 VNets (/25) et de tous les Subnets.	Vérification de l'absence de chevauchement de CIDR. Nom *AzureBastionSubnet* obligatoire.
Peering VNet	2. Configuration du Peering bidirectionnel (Hub \leftrightarrow Prod/Dev).	S'assurer des options de transit de Gateway.
Azure Bastion	3. Déploiement du service Bastion.	Bastion déroge à la Policy *Deny Public IP* pour ce service de sécurité.

Phase 3 : Services PaaS

Ressources déployées	**Ordre logique**	**Points d'attention techniques**
SQL DB et Key Vault	1. Création des instances (accès public désactivé).	Configurer l'Admin Azure AD sur les serveurs SQL.
Private Endpoints	2. Déploiement des Private Endpoints dans le *DataSubnet*.	Mise en place de la **Private DNS Zone** et liaison du VNet.
App Service	3. Création du Plan Premium V3 et de l'App Service. 4. Activation de la VNet Integration Régionale vers *WebFarmSubnet*.	L'intégration VNet doit utiliser le subnet $/26$ pour l'évolutivité.

Phase 4 : Sécurité & Administration

Ressources déployées	**Ordre logique**	**Points d'attention techniques**
NSG	1. Déploiement des NSG et association aux Subnets.	Vérifier les règles de priorité pour la communication App Service $\leftrightarrow$ Private Endpoint.
Managed Identity & KV Access	2. Activation de l'Identité Managée sur l'App Service. 3. Attribution des permissions *Get* sur le Key Vault.	Le secret SQL doit être présent dans le Key Vault.
Backups	4. Création du *Recovery Services Vault*. 5. Définition des politiques de Backup (VMs) et de Rétention (SQL).	Tester le flux de restauration pour validation.

Phase 5 : Monitoring & Alerting

Ressources déployées	Ordre logique	Points d'attention techniques
Log Analytics Workspace	1. Création du Workspace central.	S'assurer que la politique de rétention des logs est conforme.
Diagnostics	2. Activation des diagnostics des services PaaS vers le Workspace.	Configurer les métriques (CPU) et les logs applicatifs.
Alerting	3. Création du Groupe d'Actions et de la Règle d'Alerte : CPU > 80\%.	Utiliser une fenêtre d'agrégation suffisante pour éviter le *flapping*.

Phase 6 : Migration & Bascule (*Cutover*)

Ressources déployées	Ordre logique	Points d'attention techniques
Déploiement Applicatif	1. Déploiement du code (DevOps Pipeline) vers l'App Service Dev/Prod.	Les chaînes de connexion doivent utiliser le Key Vault.
Tests finaux	2. Exécution des tests d'intégration, de performance et de sécurité.	Vérifier le bon fonctionnement de la VNet Integration et des Private Endpoints.
Migration & Cutover	3. Migration des données. 4. Basculement du DNS.	Prévoir un plan de retour arrière immédiat (*rollback*) en cas d'échec.

VIII. Estimation du Coût Azure

Note : Les coûts ci-dessous sont des estimations mensuelles pour la région France Central.

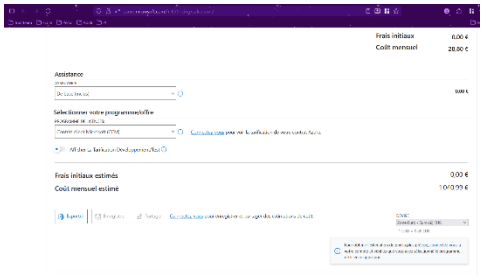
Tableau des Coûts (Estimation Mensuelle)

Composant	Tier/Taille	Coût Estimé (EUR/Mois)
App Service	Premium V3 P1v3 (x2 instances)	**280,00 €**
SQL Database	General Purpose, 2 vCores (Prod)	**250,00 €**
Storage Account	Standard GRS/LRS (5 To, Hot/Cool/Archive)	**120,00 €**
Azure Bastion	Standard	**135,00 €**
VPN Gateway	VNG1 (Base)	**150,00 €**
VMs Admin	B2s (x1, accès par Bastion)	**30,00 €**
Backups	Recovery Services Vault (500 Go)	**25,00 €**
Monitoring	Log Analytics (5 GB d'ingestion/mois)	**10,00 €**

Total Mensuel

Le **Total Mensuel Estimé** pour l'infrastructure et les services PaaS est d'environ **1000,00€**.

Lien Azure Calculator : https://azure.com/e/4fcaf3faa5214fa48e22a725200da448



IX. Feuille de Route de Migration (Roadmap)

Phase	Durée Estimée	Objectifs et Tâches Clés	Livrables
Phase A : Évaluation	1 Semaine	Recueil des exigences et identification des dépendances.	Document d'exigences (RTO, RPO, SLA).
Phase B : Conception	2 Semaines	Finalisation du plan d'adressage IP et choix des SKU PaaS.	Rapport d'Architecture complet (ce document).
Phase C : Déploiement du Socle	3 Semaines	Déploiement de la Gouvernance et du Réseau (VNets, Peering, Bastion, NSG).	Environnement réseau prêt et sécurisé.
Phase D : Mise en place PaaS	3 Semaines	Déploiement de SQL, KV, Storage, Private Endpoints, App Services, VNet Integration.	Services PaaS opérationnels et connectés en privé.
Phase E : Tests	2 Semaines	Tests d'intégration, de performance et validation du monitoring.	Rapport de tests (Performance & Sécurité).
Phase F : Migration	1 Semaine	Migration des données, déploiement du code final en Prod, basculement DNS.	Application en Production, accessible aux utilisateurs.
Phase G : Stabilisation	4 Semaines	Surveillance post-migration, optimisation des coûts, documentation d'opération.	Documentation d'exploitation et Plan d'optimisation des coûts.

X. Conclusion

Synthèse

L'architecture InnovTech représente une implémentation robuste des meilleures pratiques Azure, avec un accent fort sur le modèle Hub-and-Spoke, l'adoption du **PaaS** et une posture de sécurité renforcée par le Zero Trust. Le plan d'adressage a été structuré efficacement pour l'évolutivité.

Points Clés de Sécurité

- **Isolation Réseau :** Utilisation systématique des Private Endpoints pour tous les services de données sensibles.
- **Administration Sécurisée :** L'accès RDP/SSH est centralisé et contrôlé par **Azure Bastion**.
- **Identité Forte :** MFA et PIM sont obligatoires pour les administrateurs.
- **Gouvernance :** Azure Policy interdit les IP publiques et restreint les régions de déploiement.

Risques Majeurs et Atténuations

Risque majeur	**Mitigation**
Échec du Peering (*Overlap CIDR*)	Double vérification du plan d'adressage (Phase B) et utilisation de l'Infrastructure as Code (IaC).
Défaillance de l'App Service (Surcharge)	Configuration de l'Autoscale et de l'alerte **CPU $> 80\%$** via Azure Monitor.
Manque de résolution DNS privée	Déploiement obligatoire des **Private DNS Zones** liées aux VNets pour la résolution des Private Endpoints.