Compte Rendu Détaillé du Projet : Migration vers un Service Cloud Hybride

Période : Février 2024 - Mai 2024

Durée : 4 mois

**1. Contexte et Objectifs**

Objectif principal : Migrer une partie de l’infrastructure informatique vers un cloud hybride (AWS/Azure) en garantissant la continuité des services, la sécurité des données, et l’optimisation des coûts.

Livrables attendus :

- Analyse des besoins et choix du fournisseur cloud (AWS ou Azure).

- Déploiement d’un VPN site-to-cloud (WireGuard ou OpenVPN).

- Tests d’intégration et de performance sous charge.

- Formation des équipes et support post-migration.

Contraintes :

- Minimiser les interruptions de service pendant la migration.

- Respect des normes de sécurité (RGPD, ISO 27001).

**2. Méthodologie et Organisation**

Rôles de l’équipe :

| Rôle | Responsabilités |

|-------------------------|----------------------------------------------------|

| Chef de Projet | Coordination globale et gestion des risques. |

| Architecte Cloud | Choix du fournisseur, design de l’architecture. |

| Ingénieur Réseau | Déploiement et configuration du VPN. |

| DevOps | Automatisation des déploiements (IaC). |

| Formateur | Création des modules de formation utilisateurs. |

Outils utilisés :

- Cloud Provider : AWS (EC2, S3) / Azure (VM, Blob Storage).

- VPN : WireGuard (léger et performant) ou OpenVPN (pour compatibilité étendue).

-IaC : Terraform pour l’infrastructure as code.

- Tests de charge : JMeter et Gatling.

- Monitoring : Prometheus + Grafana.

**3. Phases du Projet**

Phase 1 : Analyse des besoins et choix du fournisseur (3 semaines)

- Étude comparative AWS vs Azure :

- AWS : Avantages en scalabilité, coûts compétitifs pour les charges variables.

- Azure : Intégration native avec les outils Microsoft (Active Directory, Office 365).

- Choix final : Azure (pour l’écosystème Microsoft existant).

- Plan de migration :

- Priorisation des applications (d’abord les services non critiques : site web, sauvegardes).

Phase 2 : Déploiement du VPN site-to-cloud (2 semaines)

- Configuration WireGuard :

- Serveur cloud (Azure VM Ubuntu) : `wg genkey | tee privatekey | wg pubkey > publickey`.

- Client on-premise : Configuration des peers avec clés publiques/privées.

- Test de débit : 950 Mbps en moyenne (vs 700 Mbps pour OpenVPN).

- Sécurisation :

- Restriction des accès via NSG (Network Security Groups) sur Azure.

Phase 3 : Migration des applications (6 semaines)

- Stratégie lift-and-shift :

- Migration des VM locales vers Azure avec Azure Migrate.

- Adaptation des applications pour le cloud (ex: remplacement des bases de données par Azure SQL).

- Automatisation :

- Scripts Terraform pour déployer les ressources (exemple : déploiement d’un conteneur AKS).

```hcl

resource "azurerm\_kubernetes\_cluster" "aks" {

name = "aks-cluster"

location = "France Central"

resource\_group\_name = azurerm\_resource\_group.rg.name

dns\_prefix = "aks"

default\_node\_pool {

name = "default"

node\_count = 3

vm\_size = "Standard\_D2\_v2"

}

}

```

Phase 4 : Tests d’intégration et de charge (2 semaines)

- Tests fonctionnels :

- Vérification de la connectivité entre les systèmes on-premise et cloud (ex: accès à une base de données hybrides).

- Tests de charge :

- Simulation de 1 000 utilisateurs simultanés sur le site web migré :

- Temps de réponse moyen : 1,2s (objectif atteint).

- Goulot d’étranglement identifié : Optimisation du cache Redis.

Phase 5 : Formation et support post-migration (3 semaines)

- Formation utilisateurs :

- Ateliers en présentiel : Gestion des ressources cloud via le portail Azure.

- Tutoriels vidéo : Surveillance des coûts avec Azure Cost Management.

- Support niveau 2 :

- Résolution des incidents liés aux latences (optimisation des requêtes SQL).

- Mise en place d’un canal Slack dédié aux questions techniques.

**4. Résultats et Livrables**

Infrastructure migrée:

- 80 % des applications critiques hébergées sur Azure.

- Coûts réduits de 25 % grâce à l’autoscaling et aux réservations Azure.

Performances :

- VPN WireGuard opérationnel avec une disponibilité de 99,98 %.

- Temps de réponse des applications amélioré de 30 %.

Documentation :

- Guide d’administration Azure (50 pages).

- Procédures de rollback en cas d’échec.

**5. Défis Rencontrés et Solutions**

| Défi | Solution |

|-----------------------------------|-----------------------------------------------|

| Latence élevée entre on-premise et cloud | Optimisation des routes BGP et déploiement d’Azure ExpressRoute. |

| Erreurs de compatibilité des applications | Refactoring partiel avec conteneurisation Docker. |

| Dépassement de budget initial | Négociation d’un contrat de réservation Azure (économies sur 3 ans). |

**6. Bilan et Perspectives**

Points forts :

- Migration transparente avec zéro interruption majeure.

- Sécurité renforcée via chiffrement AES-256 et MFA.

Améliorations futures :

- Migration des 20 % d’applications restantes (ERP legacy).

- Implémentation d’un SIEM cloud-native (Azure Sentinel).

**Annexes**

1. Architecture cloud hybride : Schéma des flux entre on-premise et Azure.

2. Script Terraform : Exemple de déploiement d’une VM Windows.

3. Rapport de tests de charge : Graphiques de performance JMeter.