Technologies Cloud et Sécurité - AZURE - Partie III

Anis Hanniz

30 novembre 2024

Table des matières

1 Concepts Fondamentaux de la Conteneurisation

1.1 Conteneurs

Les conteneurs sont des unités logicielles autonomes qui encapsulent le code et toutes ses dépendances. Ils permettent une exécution cohérente et fiable dans différents environnements informatiques.

1.2 PODS

Les PODS représentent la plus petite unité déployable dans un environnement Kubernetes. Ils peuvent contenir un ou plusieurs conteneurs qui partagent les mêmes ressources, notamment le stockage et le réseau.

1.3 Nodes (VM)

Un Node, équivalent à une machine virtuelle, est un composant d'un cluster Kubernetes sur lequel s'exécutent les pods. Il fournit l'environnement d'exécution nécessaire.

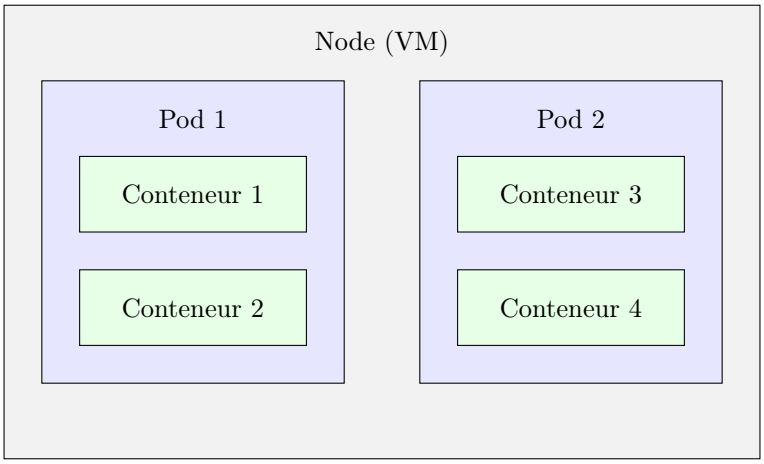

Figure 1 – Architecture d'un Node avec Pods et Conteneurs

Résumé du Processus de Migration Cloud

Cette section présente une vue d'ensemble du processus de migration et de l'architecture cible pour une infrastructure hybride cloud.

Processus de Migration

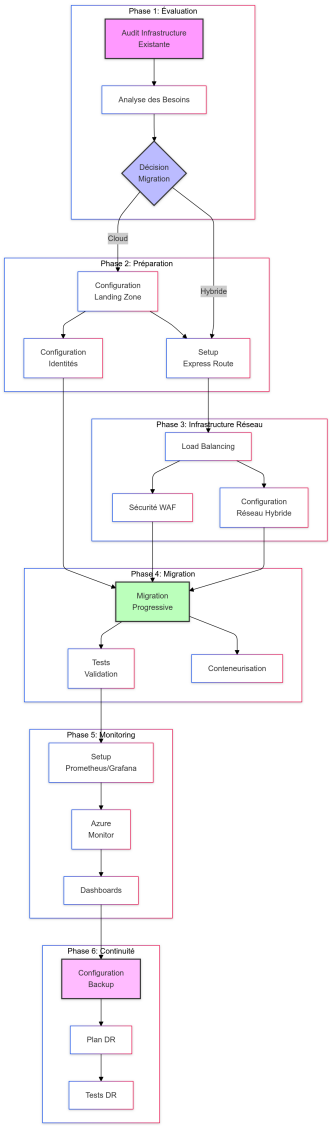

FIGURE 2 – Processus complet de migration vers le cloud

Le diagramme ci-dessus illustre les différentes phases de migration, de l'évaluation initiale jusqu'à la mise en place des mécanismes de continuité d'activité. Chaque phase est interconnectée et permet une transition progressive vers le cloud.

Architecture Hybride Cible

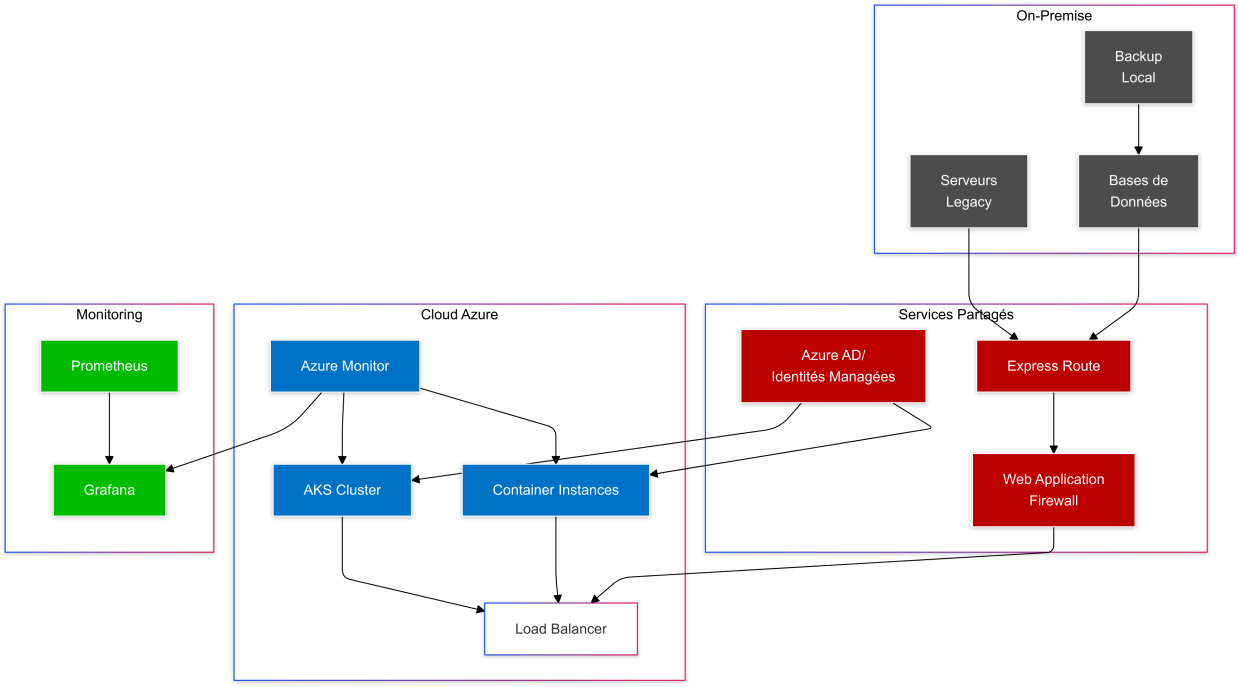

FIGURE 3 – Architecture hybride cloud-onpremise

Cette architecture présente l'organisation finale d'une infrastructure hybride type, montrant l'interconnexion entre :

— Les services cloud Azure (AKS, ACI)

— Les services partagés (Express Route, WAF)

— L'infrastructure on-premise existante

— La solution de monitoring globale

2 Patterns de Communication

Voir : https ://anishanniz.github.io/sync-problems-visualization/

2.1 Modèle Producteur-Consommateur

Architecture où des processus producteurs génèrent des données qui sont ensuite traitées par des processus consommateurs. Ce modèle permet une séparation efficace des responsabilités.

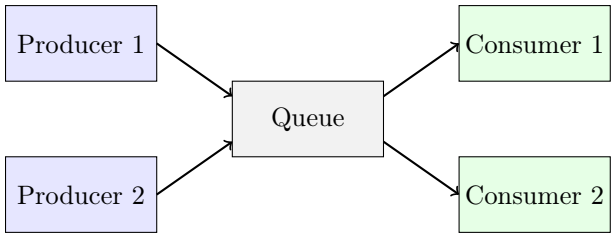

FIGURE 4 – Modèle Producteur-Consommateur

2.2 Exclusion Mutuelle (Mutex / Sémaphores)

Mécanisme de synchronisation empêchant l'accès simultané à une ressource partagée par plusieurs processus, garantissant ainsi l'intégrité des données.

3 Solutions de Conteneurisation Cloud

3.1 Services Conteneurisés Simplifiés

3.1.1 ACA/ECA/GCA

Versions simplifiées de Kubernetes proposées respectivement par Azure, AWS et Google Cloud, offrant une expérience plus accessible.

3.1.2 ACI (Azure Container Instances)

Service Azure permettant l'exécution de conteneurs sans nécessiter la gestion de l'infrastructure sous-jacente.

3.1.3 AKS (Azure Kubernetes Service)

Service Kubernetes entièrement géré par Azure, simplifiant le déploiement et la gestion des applications conteneurisées.

3.1.4 TANZU

Plateforme VMware dédiée à la modernisation des applications et à la gestion des conteneurs dans un environnement d'entreprise.

4 Infrastructure Réseau et Sécurité

4.1 Solutions de Load Balancing

4.1.1 Load Balancer Standard

Système de répartition de charge distribuant le trafic entre différents serveurs pour optimiser les ressources. Cette solution permet la mise en place d'une architecture multi-environnements, exemple :

— PROD : Environnement de production destiné aux utilisateurs finaux
— HORS PROD : Environnement de recette et de tests internes
— SUPPORT : Environnement dédié au support et à la maintenance

4.1.2 Load Balancer Niveau 7 avec WAF

Solution de répartition de charge au niveau applicatif intégrant un pare-feu pour applications web (WAF). Cette architecture permet de :

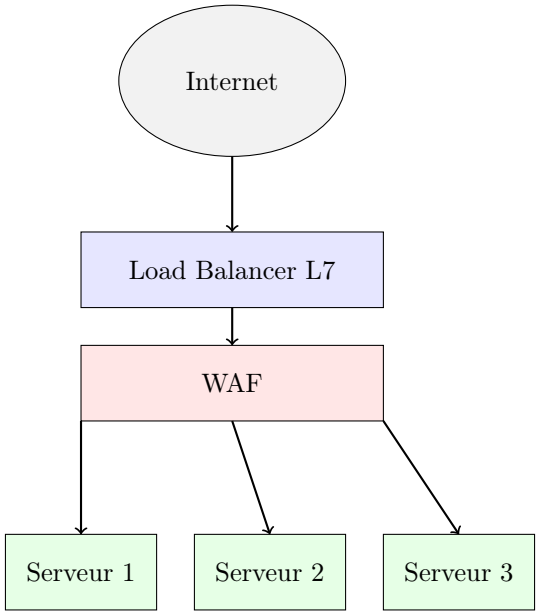

FIGURE 5 – Architecture Load Balancer niveau 7 avec WAF

— Router le trafic vers l'environnement approprié selon l'URL d'entrée
— Appliquer des politiques de sécurité différenciées
— Gérer des certificats SSL distincts par environnement
— Mettre en place des quotas et limitations de ressources spécifiques

4.1.3 HAPROXY

Solution open-source de load balancing et de proxy haute performance, permettant une configuration fine des règles de routage et de la gestion des sessions par environnement.

4.2 Sécurité et Contrôle d'Accès

4.2.1 OWASP

Organisation définissant les standards et bonnes pratiques de sécurité pour les applications web.

4.2.2 Ingress Controller

Composant Kubernetes gérant le trafic entrant dans le cluster.

4.2.3 Redirections URL

Mécanisme permettant de rediriger les requêtes d'une URL vers une autre.

4.2.4 Offload SSL

Technique de délégation du chiffrement SSL à un équipement spécialisé.

4.3 Connectivité

4.3.1 Express Route

Service de connexion privée dédiée entre l'infrastructure on-premises et Azure.

5 Monitoring et Observabilité

5.1 Outils de Surveillance

5.1.1 Prometheus

Système open-source de surveillance et d'alerte pour environnements conteneurisés.

5.1.2 Grafana

Plateforme de visualisation pour métriques et logs.

5.2 Solutions Azure

5.2.1 Azure Monitor

Service de surveillance intégré d'Azure.

5.2.2 Azure Analytics Workspace

Service d'analyse de logs centralisé.

5.2.3 .NET Aspire Dashboard

Interface de monitoring spécifique aux applications .NET Aspire.

5.3 Architecture de Monitoring

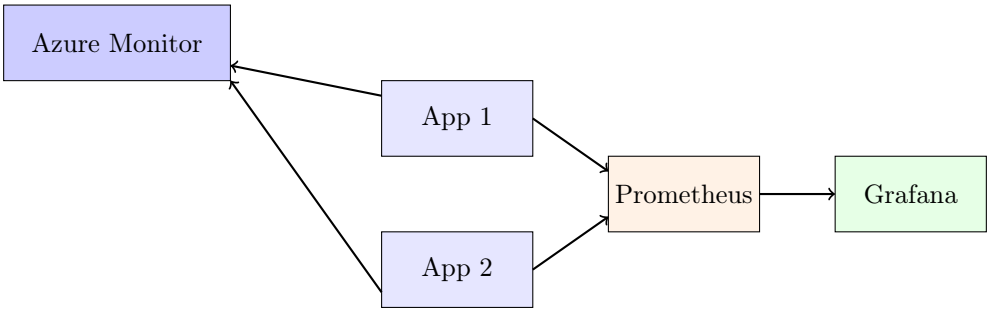

Figure 6 – Architecture de Monitoring

6 Infrastructure et Migration

6.1 Landing Zone

Infrastructure cloud préparée et sécurisée pour accueillir les workloads d'entreprise.

6.2 Environnement Staging

Environnement de pré-production permettant de tester les applications avant leur déploiement en production.

6.3 Move2Cloud

Stratégie et méthodologie de migration des applications vers le cloud.

7 Gestion des Identités

7.1 Identités Managées

Service Azure automatisant la gestion des identités des ressources cloud.

8 Sauvegarde et Restauration

8.1 Solutions de Backup

8.1.1 Recovery Services Vault

Service Azure centralisant les sauvegardes et la restauration.

8.1.2 Veeam Kasten

Solution spécialisée pour la sauvegarde d'applications Kubernetes.

8.1.3 Portworx PX-Backup

Solution de sauvegarde conçue pour les applications cloud-natives.