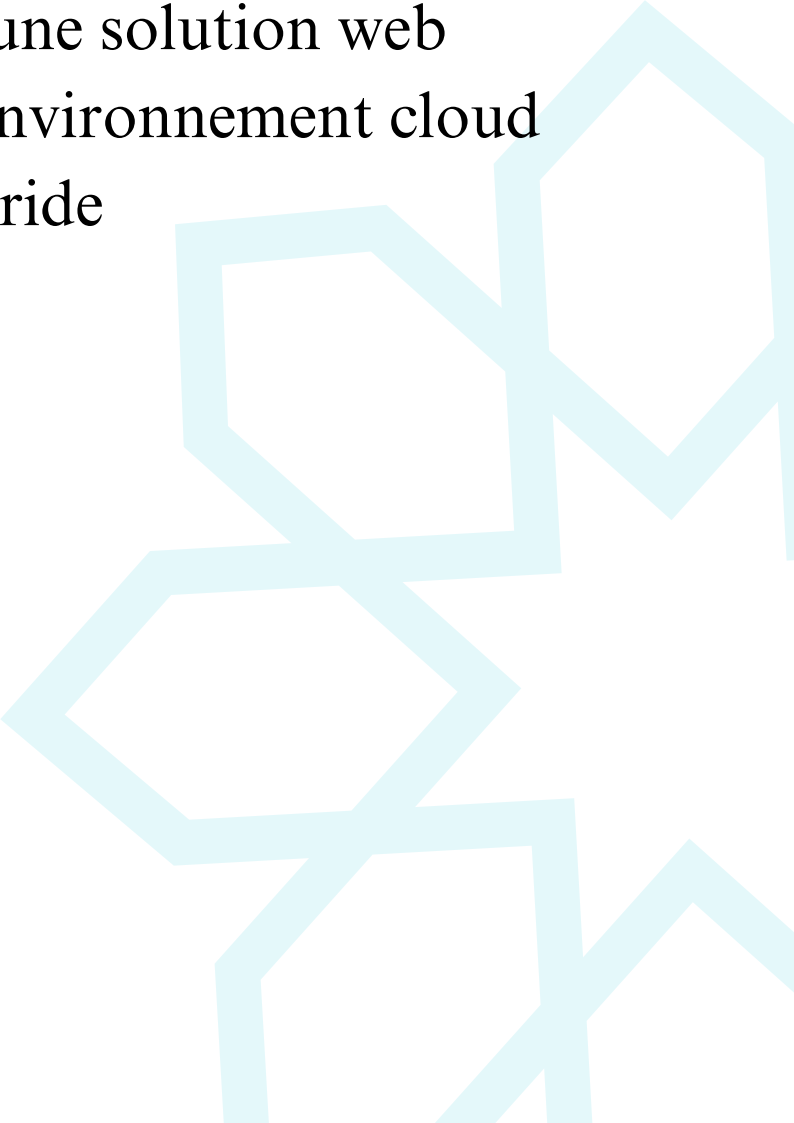


Solution Cloud Hybride (CESE)

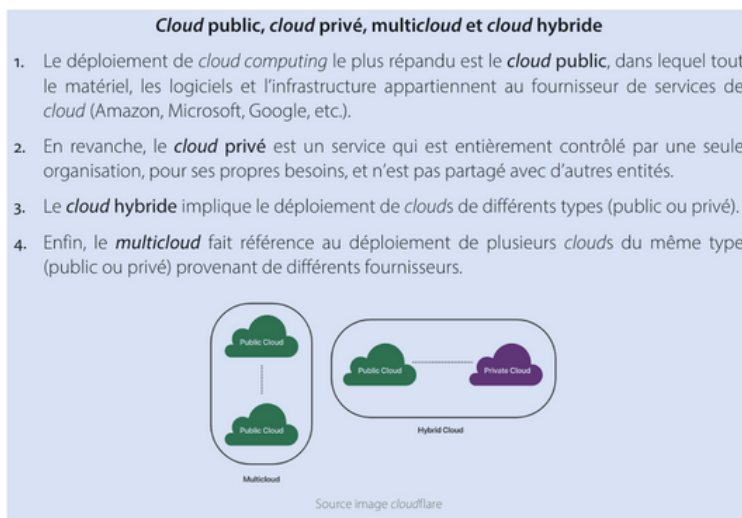
Mise en place d'une solution web
dynamique sur un environnement cloud
hybride



Introduction

Le déploiement d'une solution web dynamique dans un environnement cloud hybride permet aux institutions gouvernementales de tirer parti des avantages des infrastructures publiques et privées pour offrir des services numériques sécurisés et performants. Ce document explore comment cette approche hybride peut être utilisée pour sécuriser et optimiser des portails web gouvernementaux, tout en respectant les normes de conformité strictes.

<https://www.ibm.com/fr-fr/think/insights/hybrid-cloud-advantages-disadvantages>



<https://tawssia.ma/>

Les Enjeux du Cloud Hybride

Objectifs et Avantages

Flexibilité : Permet de migrer les charges de travail des applications web entre les environnements cloud en fonction des besoins de sécurité et de performance.

Évolutivité : Capacité à gérer les fluctuations de trafic sur les services en ligne gouvernementaux.

Sécurité : Utilisation du cloud privé pour stocker et traiter les données sensibles, garantissant ainsi la conformité réglementaire et la protection des informations citoyennes.

Continuité des services : Assure une disponibilité constante des services web, essentielle pour la confiance publique.

Défis et Risques

Sécurité des données : Les données des citoyens doivent être protégées des fuites, des cyberattaques et des mauvaises configurations.

Latence réseau : Cruciale pour l'expérience utilisateur des services web publics.

Interopérabilité : Nécessaire pour intégrer les systèmes internes avec les services cloud externes sans compromettre la sécurité.

Conformité réglementaire : Respect des normes comme le RGPD, la loi sur la confidentialité des données, etc., pour les applications web gouvernementales.

<https://www.ibm.com/fr-fr/think/insights/hybrid-cloud-advantages-disadvantages>

Benchmarks et Meilleures Pratiques pour la Solution Web Gouvernementale:

Catégorie	Benchmark	Description	Applicable à
Sécurité Générale	OWASP Cloud Security	Guide pour sécuriser les applications web sur le cloud.	Cloud, SaaS, API pour web gouvernemental
	CIS Benchmarks	Standards de configuration sécurisée spécifiques aux environnements cloud hybrides utilisés par les institutions publiques.	Toutes plateformes cloud
Performance Réseau	iPerf	Mesure la performance réseau pour assurer une expérience utilisateur optimale sur les plateformes web gouvernementales.	Réseaux cloud hybrides
Stockage & IOPS	FIO	Teste les performances de stockage pour les bases de données critiques à la gestion des données citoyennes.	SSD, stockage cloud pour applications
Performances des VM	Geekbench	Évalue la performance des machines virtuelles hébergeant les applications web gouvernementales.	VMs et serveurs web
Bases de Données	TPC-C	Benchmark des performances transactionnelles SQL pour les applications web de services publics.	Bases de données pour applications web
Applications & API	Apache JMeter	Simulation de charge pour tester la scalabilité et la robustesse des applications web gouvernementales.	Web, SaaS, microservices

<https://en.wikipedia.org/wiki/PerfKitBenchmarker>

<https://cloud.google.com/blog/products/networking/perfkit-benchmark-for-evaluating-cloud-network-performance>

https://pages.awscloud.com/rs/112-TZM-766/images/Frost_Sullivan_Global_Cloud_Radar_and_IaaSaaS_Market_Update_2021.pdf

Étude de Cas :

Infrastructure : Utilisation de OpenStack pour le cloud privé et Azure pour le cloud public, connectés via Azure ExpressRoute.

Sécurité : Implémentation des recommandations OWASP, CIS Benchmarks, et respect des normes NIST 800-53 pour garantir la sécurité des données.

Performance : Évaluation continue avec iPerf pour la connectivité réseau et FIO pour les performances de stockage.

Résultats : Amélioration notable de la latence et une sécurité renforcée des services en ligne.

- Informations sur Azure ExpressRoute et Azure VPN Gateway : [Microsoft Learn](#)
- Informations sur AWS Direct Connect : [AWS Documentation](#)
- Informations sur Google Cloud Interconnect : [Google Cloud Docs](#)
- Scores de sécurité : [Gartner](#), [Forrester](#), [IDC](#), [Cybersecurity Insiders](#) , [CIS](#) , [NIST](#)

Meilleures Pratiques de Sécurité pour le Cloud Hybride:

Automatisation : Utilisation d'outils comme Terraform pour gérer des configurations de sécurité cohérentes.

Audits Réguliers : Pour détecter les failles et assurer la conformité.

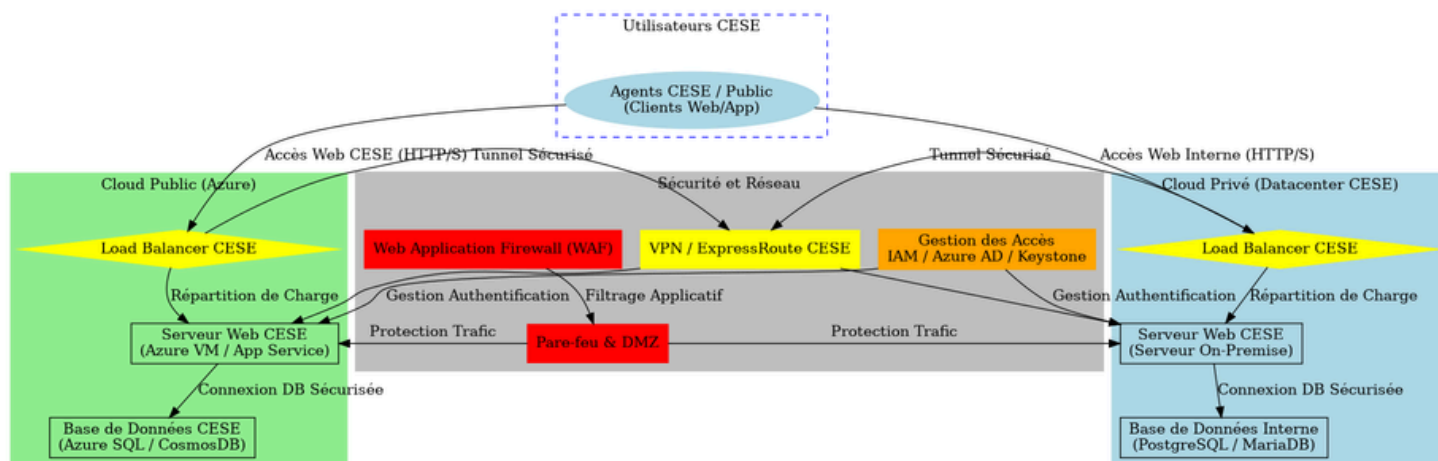
Politiques de Sécurité Standardisées : Adhésion aux cadres comme NIST et CIS.

Chiffrement des Données : Utilisation de TLS et KMS pour protéger les données en transit et au repos.

Sécurité des Points d'Accès : Authentification multi-facteurs et outils EDR.

Contrôle d'Accès Basé sur les Rôles (RBAC) : Pour limiter l'accès aux ressources critiques.

Ce schéma respecte les critères définis pour la mise en place d'une solution web dynamique sur un environnement cloud hybride

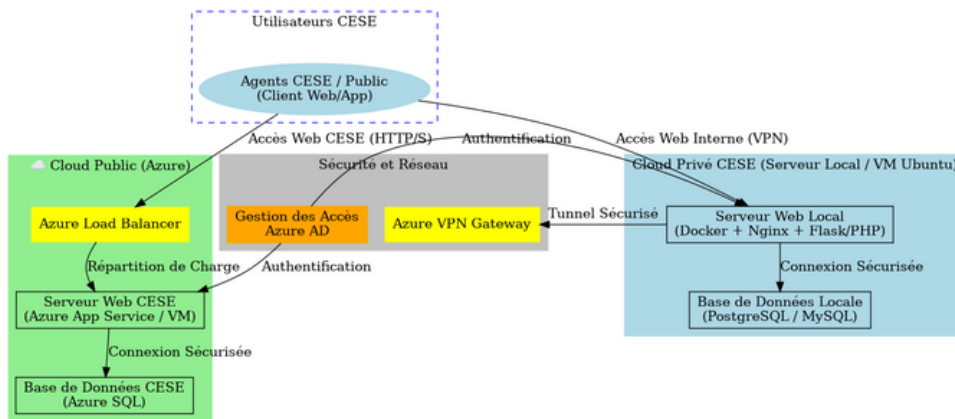


Réalisé par : Abderrahim Bouallaga stagiaire IT Cloud
Date : 2/20/2025

Architecture Hybride Cloud CESE

Ce schéma représente une infrastructure hybride combinant OpenStack (Cloud Privé) et Azure (Cloud Public) via ExpressRoute pour une connectivité sécurisée et performante. La sécurité est renforcée par un pare-feu, un WAF et une DMZ, tandis que l'authentification est gérée via IAM, Azure AD et Keystone. La répartition de charge est assurée par des load balancers des deux côtés, avec une connexion sécurisée aux bases de données. Cette architecture garantit une haute disponibilité et une protection avancée des données.

Schéma Simplifié : Solution Web Dynamique sur un Cloud Hybride pour le test pratique



Réalisé par : Abderrahim Bouallaga stagiaire IT Cloud
Date : 2/20/2025

Perspectives et Évolutions Futures du Cloud Hybride

L'avenir du cloud hybride est marqué par des avancées technologiques et des évolutions stratégiques majeures. Parmi les tendances à surveiller :

Expansion des Regions Cloud en Afrique : l'intérêt croissant pour le cloud en Afrique pousse des fournisseurs comme Microsoft Azure, AWS et Google Cloud à envisager l'ouverture de nouvelles régions. Si Azure implémente une région au Maroc, cela réduirait la latence et améliorerait la conformité aux réglementations locales.

Développement des Solutions Souveraines : Les gouvernements et entreprises recherchent des solutions cloud souveraines pour garantir la protection des données sensibles et la conformité aux réglementations locales.

Émergence du Cloud Distribué : L'adoption du cloud distribué permet une gestion plus fluide des ressources entre infrastructures privées et publiques tout en optimisant la performance et la sécurité.

Renforcement des Standards de Sécurité : L'intégration de nouvelles normes et protocoles renforcera la résilience face aux cybermenaces et aux attaques avancées.

Conclusion

L'adoption d'un cloud hybride pour les applications web gouvernementales offre une voie vers des services numériques plus sécurisés, performants et conformes. Cette approche garantit non seulement une meilleure gestion des ressources mais aussi une protection renforcée des données publiques.

Sources et Références

<https://csrc.nist.gov/publications>

<https://learn.microsoft.com/en-us/security/>

<https://www.redhat.com/en/blog/hybrid-cloud-platform-layers>

<https://www.vmware.com/topics/hybrid-cloud-architecture>

<https://learn.microsoft.com/en-us/azure/defender-for-cloud/concept-regulatory-compliance>

<https://learn.microsoft.com/en-us/azure/defender-for-cloud/secure-score-security-controls>

