Recherche & Benchmarks du Cloud Hybride (CESE)

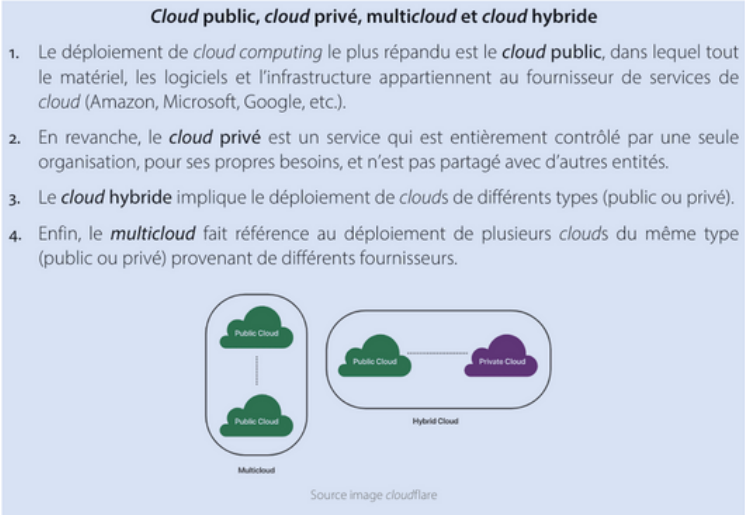
Analyse des Benchmarks pour l'Évaluation des Performances et de la Sécurité d’un Cloud Hybride

Introduction

Le cloud hybride est une conception d'infrastructure informatique qui intègre les ressources informatiques internes d'une entreprise avec l'infrastructure et les services de fournisseurs de cloud tiers. Avec le cloud hybride, vous pouvez stocker vos données et exécuter vos applications dans de multiples environnements. Votre environnement de cloud hybride vous aide à mettre en service, à mettre à l'échelle et à gérer de façon centralisée vos ressources informatiques.

L'objectif de cette recherche est d'explorer les benchmarks les plus pertinents pour un cloud hybride, en couvrant aussi bien les performances réseau, de stockage, de virtualisation, de bases de données que les aspects de sécurité

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



https://tawssia.ma/

Les Enjeux du Cloud Hybride

Avantage du Cloud Hybride

Flexibilite: possibilite de repartir les charges de travail entre differents environnemants

Evolutivite: adaptation rapide aux besoins en ressources

Optimisation des couts: utilisation dun cloud public pour les charges variables et dun cloud prive pour les operations sensibles

Continuite des services: resilience accrue grace a la redondance des inf

Défis et Risques

Securite des donnees: risques lies aux fuites, a la mauvaise configuration des services et aux cyberattaques.

Latence reseau: performance variable selon la connexion entre les infrastructures.

Interoperabilite: compatibilite des sevices et des API entre les differents fournisseurs .

Conformite reglementaire: necessite de respecter les normes en vigueur (RGPD,ISO 27001 , ect.).

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

Catégories de Benchmarks pour le Cloud Hybride:

Catégorie	Benchmark	Description	Applicable à
Sécurité Générale	CIS Benchmarks	Standards de configuration sécurisée pour OS, cloud, etc.	Toutes plateformes (AWS, Azure, GCP, OpenStack, VMware)
	NIST 800-53	Cadre de contrôle de sécurité pour infrastructures IT.	Secteur public, entreprises
	ISO 27001	Norme de gestion de la sécurité de l'information.	Cloud hybride, organisations
	OWASP Cloud Security	Évaluation des risques liés aux applications cloud.	Cloud, SaaS, API
Performance Réseau	iPerf	Test de bande passante et latence réseau.	Réseaux cloud hybrides
	Netperf	Évaluation du débit et de la latence TCP/UDP.	Réseaux multi-cloud
	Ping & Traceroute	Mesure de la latence et des sauts réseau.	Toute interconnexion réseau
Stockage & IOPS	FIO (Flexible I/O Tester)	Teste les performances des disques (latence, débit).	SSD, HDD, stockage cloud
	IOzone	Benchmark des systèmes de fichiers (lecture/écriture).	Stockage cloud hybride
Sécurité des VM	Lynis	Audit de sécurité pour Linux et OpenStack.	Machines virtuelles (VMs)
	Microsoft Defender for Cloud	Analyse de menaces sur les environnements cloud.	Multi-cloud (AWS, Azure, GCP)
	AWS Security Hub	Évalue la sécurité des ressources AWS.	AWS uniquement
Performances des VM	Geekbench	Teste la puissance CPU et mémoire.	VMs et serveurs physiques
	Sysbench	Évalue CPU, mémoire, stockage et BDD.	Cloud et On-Premises
	SPEC CPU	Benchmark des performances des processeurs.	Datacenters, cloud providers
Bases de Données	TPC-C / TPC-H	Benchmark des performances transactionnelles SQL.	Bases de données SQL/NoSQL
	HammerDB	Test de performance des bases de données.	MySQL, PostgreSQL, SQL Server
Applications & API	Apache JMeter	Simulation de charge sur applications et API.	Web, SaaS, microservices
	K6 (Load Impact)	Benchmark des performances d'API et de services web.	API REST, GraphQL

https://en.wikipedia.org/wiki/PerfKitBenchmarker
https://cloud.google.com/blog/products/networking/perfkit-benchmarker-for-evaluating-cloud-network-performance
https://pages.awscloud.com/rs/112-TZM-766/images/Frost_Sullivan_Global_Cloud_Radar_and_IaaSPaaS_Market_Update_2021.pdf

Chaque benchmark répond à des besoins spécifiques :

- Sécurité : CIS et NIST 800-53 adaptés aux exigences gouvernementales.
- Réseau : iPerf privilégié pour mesurer la connectivité inter-cloud.
- Stockage : FIO recommandé pour les infrastructures hautes performances.
- Virtualisation : Geekbench et Sysbench utiles pour ajuster les performances des machines virtuelles.

Étude de Cas et Recommandations

Cas d'Usage : Déploiement Sécurisé d'un Cloud Hybride

- Infrastructure : OpenStack (privé) et Azure (public) interconnectés via ExpressRoute.
- Sécurité : Implémentation des recommandations CIS Benchmarks et NIST 800-53.
- Performance : Évaluation avec iPerf pour la connectivité et IOzone pour le stockage.
- Résultats : Amélioration de la latence et renforcement des contrôles de sécurité.

Meilleures Pratiques de Sécurité pour le Cloud Hybride

Automatisation pour la Sécurité L'automatisation joue un rôle crucial dans le maintien de la securite en garantissant des politiques cohérentes et une réponse rapide aux menaces. Des outils comme Terraform et AWS CloudFormation permettent d'appliquer des configurations de sécurité, tandis que le patching et la surveillance automatisés facilitent les opérations.

Audits Réguliers Les audits sont essentiels pour identifier les mauvaises configurations et les problèmes d'accès. La revue des permissions et l'utilisation des outils d'audit des fournisseurs cloud permettent d'éviter les accès non autorisés et les failles de sécurité.

Politiques de Sécurite Standardisées Suivre des cadres de référence comme les CIS Benchmarks ou le NIST Cybersecurity Framework assure une protection uniforme entre les clouds privés et publics.

Chiffrement et Sauvegardes des Données Le chiffrement des données au repos et en transit avec TLS et KMS empêche l'accès non autorisé, tandis que des sauvegardes sécurisées garantissent la récupération en cas d'incident.

Sécurité des Points d'Accès Les points d'acces doivent être protégés avec des outils de détection et de réponse aux menaces (EDR) ainsi que l'authentification multi-facteurs (MFA) pour réduire les risques.

Contrôle d'Accès Basé sur les Rôles (RBAC) Le RBAC limite l'accès en fonction des rôles des utilisateurs, réduisant ainsi les risques de modifications non autorisées. Des outils comme AWS IAM ou Azure Active Directory facilitent la gestion sécurisée des rôles.

Interopérabilité Sécurisée Garantir l'interopérabilité entre les services cloud via des API standardisées et sécurisées permet un échange de données fluide et protégé.
En adoptant ces bonnes pratiques, les organisations peuvent renforcer la sécurité de leur infrastructure cloud hybride, atténuer les risques et garantir la conformité.

Configuration des Clouds Hybrides et Évaluation de la Sécurité

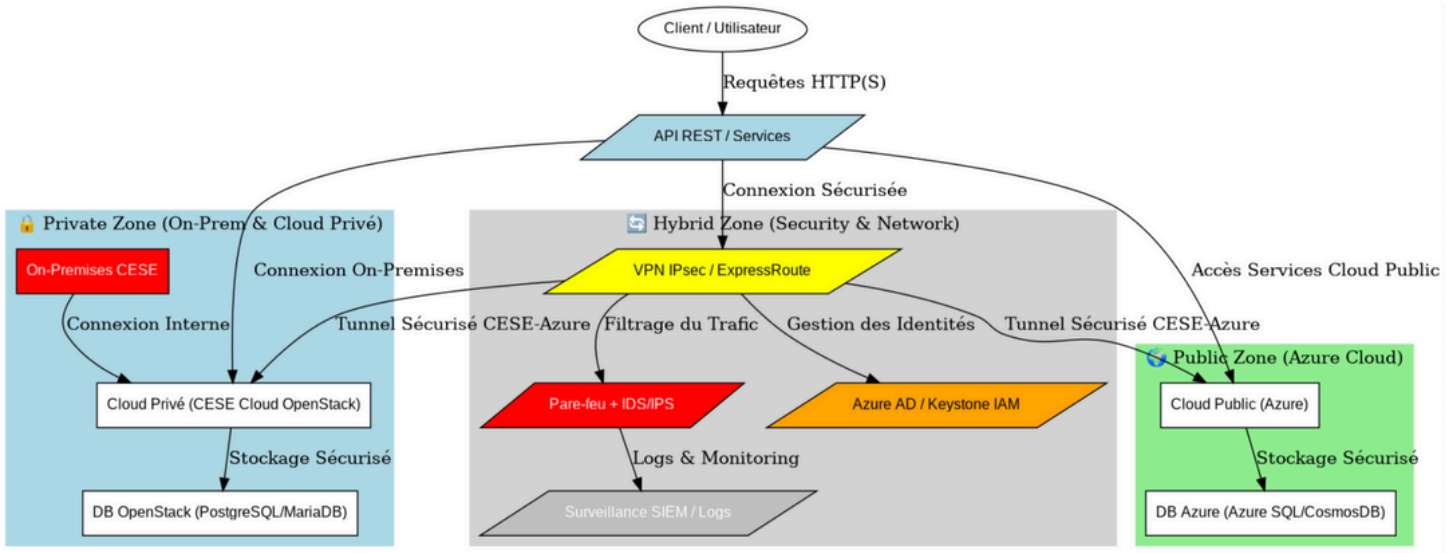
Configuration	Cloud Privé	Cloud Public	Connectivité	Sécurité Mondiale (Score sur 10)
Option 1	OpenStack	Azure	Azure ExpressRoute	9.2/10
Option 2	VMware vSphere	AWS	AWS Direct Connect	9.1/10
Option 3	Proxmox	Google Cloud	VPN IPsec	7.5/10
Option 4	Nutanix	Google Cloud	Google Cloud Interconnect	9.0/10

Comparaison des Solutions de Connectivité pour le Cloud Hybride

Solution	Fiabilité	Performance Réseau	Coût
Azure ExpressRoute	Élevée	Très bonne	Élevé (frais de port, bande passante, maintenance)
Azure VPN Gateway	Moyenne	Bonne	Moyen (coût de gestion et consommation)
AWS Direct Connect	Élevée	Très bonne	Élevé (similaire à ExpressRoute)
Google Cloud Interconnect	Élevée	Très bonne	Élevé (coût comparable aux autres solutions directes)

- 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

Réalisation théorique de l'architecture de sécurité d'un cloud hybride basé sur OpenStack (privé) et Azure (public)



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 reduirait la latence et améliorerait la conformité aux reglementations 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 Distribue : 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'integration de nouvelles normes et protocoles renforcera la résilience face aux cybermenaces et aux attaques avancées.

Conclusion

Le cloud hybride garanti une performance et une securite optimales . l'integration de standards reconnus et l'adoption d'outils de mesure precis permettent aux entreprises de securiser leurs infrastructures tout en maximisant leur efficacite . un suivi regulier et des test continus sont indispensables pour adaptation aux evolutions technologiques et reglementaires.

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