FR

# Guide Multi-Cloud PME

## Eviter le vendor lock-in sans complexite

Terraform, Kubernetes multi-cluster, identite federee — cas BOTUM

**AWS** + **Azure** + **GCP**

Mars 2026

## Introduction : le multi-cloud, une realite operationnelle

Selon le rapport Flexera State of the Cloud 2024, 70% des entreprises utilisent desormais deux clouds publics ou plus. Parmi les PME, ce chiffre est souvent le resultat d'une accumulation organique plutot que d'une decision strategique : un SaaS critique sur AWS, une infrastructure Azure pour M365, un projet pilote IA sur GCP. Ce guide est pour les CTOs et DevOps qui veulent passer du multi-cloud accidentel au multi-cloud maitrise.

## Pourquoi les PME deviennent multi-cloud sans le decider

- Integration SaaS : Salesforce (AWS), Teams (Azure), BigQuery (GCP) — chaque outil sur son cloud
- Heritage historique : migration Azure pour AD, puis SageMaker pour le ML, puis BigQuery pour la data
- Acquisitions : la startup rachetee tourne sur GCP — migration = 18 mois
- Projets pilotes permanents : 'on teste juste GCP pour l'IA' — 2 ans apres, c'est en prod

## Multi-cloud intentionnel vs accidentel

### Multi-cloud accidentel :

- ✗ Absence de gouvernance centrale — personne ne sait tout ce qui tourne
- ✗ Identites gerees en silo dans chaque provider
- ✗ Couts difficiles a attribuer — egress fees invisibles
- ✗ Securite fragmentee — vision incomplete

### Multi-cloud intentionnel :

- ✓ Chaque cloud choisi pour ce qu'il fait mieux
- ✓ Couche d'abstraction unifiee (Terraform, Kubernetes)
- ✓ Identites federees — un login partout
- ✓ Couts visibles et maitrisés — CloudHealth ou equivalent

## Les vrais benefices (quand c'est intentionnel)

### Resilience

Panne us-east-1 en dec 2021 ? Rediriger vers Azure ou GCP. Demande de la preparation, mais c'est faisable.

### Levier de negociation

Demontrez votre capacite a deplacer des workloads. Economies typiques : 20-30% sur les contrats Enterprise.

### Meilleur service par cas d'usage

AWS = compute/storage/ML. Azure = M365/identite. GCP = analytics/IA. Choisir le meilleur outil.

### Conformite et souverainete
LPRPDE, PHIPA : choisir le provider avec les meilleures garanties de residence au Canada.

## Les vrais defis (sans faux-semblants)

### Complexite operationnelle
Trois consoles, trois CLIs (aws/az/gcloud), trois modeles IAM. Une equipe de 3 DevOps peut y passer 40% de son temps sans les bons outils.

### Couts de formation
AWS + Azure + GCP certifications = 6-12 mois d'investissement par ingenieur. Ne pas sous-estimer.

### Egress fees inter-cloud
AWS/Azure/GCP facturent 8-9 cents/GB sortant. 10 TB/mois inter-cloud = 800-900 USD/mois en transferts seuls.

### Securite unifiee
AWS IAM, Azure Entra ID, GCP Cloud IAM = trois syntaxes differentes. Sans identite federee, trois systemes d'acces en silo.

## Strategies pratiques pour un multi-cloud maitrise

### 1. Abstraction layer : Terraform et Pulumi
Regle d'or : ne jamais utiliser les consoles cloud directement. Tout passe par l'IaC.

- Terraform (HashiCorp) : standard industrie. Providers AWS/Azure/GCP + 1000 autres. Modules reutilisables. Terraform Cloud ou Atlantis pour CI/CD.
- Pulumi : memes concepts, vrais langages (Python, TypeScript, Go). Ideal pour les equipes qui preferent coder en Python.
- Avantage cle : infrastructure versionnable, auditable, reproductible. Migration = changer des variables de provider.

### 2. Kubernetes multi-cluster
- EKS (AWS) + AKS (Azure) + GKE (GCP) : memes workloads containers sur les trois
- Anthos (Google) ou Rancher : gestion unifiee multi-clusters
- Azure Arc : etend la gouvernance Azure sur AWS/GCP/on-prem
- Crossplane : provisionne des ressources cloud via CRDs Kubernetes
- Istio/Linkerd : mTLS inter-cluster + routage progressif (20% AWS / 80% Azure)

### 3. Identite federee : un login pour tous les clouds
- Okta : standard Enterprise. Federe vers AWS (IAM Identity Center), Azure (Entra ID), GCP (Workforce Identity Federation)

• Azure Entra ID : si deja sur M365, solution naturelle. Federe vers AWS via SAML/OIDC et GCP via WIF

• AWS IAM Identity Center : si AWS est le cloud primaire, gere multi-comptes AWS + federation SP vers Azure/GCP

## Quand choisir quoi

### Choisissez AWS quand :

• Meilleur ecosysteme compute (EC2, ECS, EKS, Lambda)

• Stockage objet le plus mature (S3)

• Plus grand marche ML (SageMaker, Bedrock)

• Stack tech sans dependance forte a Microsoft

### Choisissez Azure quand :

• Vous utilisez M365 (Teams, SharePoint, Outlook) — integration native

• Active Directory on-prem a hybrider

• Workloads Windows Server

• Secteur reglemente canadien (OSFI, sante) qui prefere Microsoft

### Choisissez GCP quand :

• Besoins analytics importants (BigQuery imbattable au prix)

• Projets IA/ML avec TPUs et Vertex AI / Gemini

• Applications mobiles/web (Firebase)

• Besoin reseau premium faible latence

## Tableau comparatif : AWS vs Azure vs GCP

| Critere | AWS | Azure | GCP |
|---|---|---|---|
| **Compute** | EC2, ECS, EKS, Lambda, Fargate | VM, AKS, Container Apps, Functions | GCE, GKE, Cloud Run, Cloud Functions |
| **Stockage** | S3, EBS, EFS, Glacier | Blob, Disk, Files, Archive | GCS, Persistent Disk, Filestore |
| **Bases donnees** | RDS, DynamoDB, Aurora, Redshift | Azure SQL, Cosmos DB, Synapse | Cloud SQL, Spanner, Firestore, BigQuery |
| **IA / ML** | SageMaker, Bedrock, Rekognition | Azure AI, OpenAI Service, Copilot | Vertex AI, Gemini, AutoML, TPUs |
| **Identite** | IAM, IAM Identity Center | Entra ID (Azure AD), PIM | Cloud IAM, Workforce Identity Fed. |
| **Reseau** | VPC, Route53, CloudFront, WAF | VNet, DNS, Front Door, WAF | VPC, Cloud DNS, Cloud CDN, Cloud Armor |
| **IaC natif** | CloudFormation, CDK | ARM, Bicep | Deployment Manager, Config Connector |
| **Point fort PME** | Ecosysteme + market share #1 | M365 + Active Directory hybride | BigQuery + AI a la pointe |

## Outils de gestion multi-cloud

### Google Anthos
Multi-cloud et hybride Google. Gestion unifiee Kubernetes sur tous clouds + on-prem.

### Azure Arc
Etend les services Azure (governance, policy, monitoring) a AWS, GCP, on-prem, edge.

### Crossplane
Open-source CNCF. Infrastructure cloud via CRDs Kubernetes. GitOps natif.

### CloudHealth (VMware Aria)
Visibilite couts par cloud/equipe/projet. Indispensable a partir de 10k$/mois.

### Spot.io (NetApp)
Optimisation couts par IA : mix Spot/Preemptible transparent. Economies 60-80% sur batch.

## Erreurs communes a eviter

### Vouloir tout repliquer partout
Double des couts, double de la complexite, desynchronisation garantie. Architecture asymetrique, pas copier-coller.

### Sous-estimer les egress fees
Invisibles dans les estimations, devastateurs sur la facture. Regle : colocalisez les donnees avec les services qui les consomment.

### Pas de gouvernance centralisee
18 mois sans governance = 47 comptes AWS, 23 subscriptions Azure, 0 visibilite. AWS Organization + SCP des jour 1.

### Ignorer les differences IAM
AWS IAM ≠ Entra ID ≠ GCP Cloud IAM. Former les equipes sur les 3 modeles est la base de la securite multi-cloud.

### Pas de plan de sortie
Sans exercice de portabilite annuel, le vendor lock-in reste meme avec 3 providers.

## Cas concret BOTUM : SaaS PME multi-cloud maitrise
Editeur SaaS quebecois, 65 employes, 2,4M$ ARR. Situation initiale : AWS pour la prod, Azure non planifie (M365), GCP non planifie (BigQuery pilote devenu prod). Probleme : 3 clouds non gouvernes, egress fees invisibles (400$/mois BigQuery -> S3), identites en silo, aucune vue consolidee.

### Mise en place BOTUM :

• Gouvernance unifiee : AWS Organization + SCPs, Azure Management Group, GCP folder hierarchy. CloudHealth pour le billing consolide.

• Identite federee : Azure Entra ID comme IdP principal (deja M365). Federe vers AWS IAM Identity Center (SAML 2.0) + GCP Workforce Identity Federation.

• Migration donnees BigQuery : lecture GCS au lieu de S3 (job Cloud Run nocturne S3 -> GCS). Economie : 380$/mois egress.

• IaC unifie : tout Terraform, modules par cloud, state dans S3 avec locking DynamoDB.

• Monitoring unifie : Datadog comme couche observabilite commune. Metriques AWS + Azure + GCP dans un dashboard.

### Resultats apres 6 mois :

✓ Couts cloud reduits de 28% (egress + Spot.io + negociation Azure EA)

✓ MTTR incidents reduit de 45% (monitoring unifie)

✓ Onboarding nouveaux devs : 3 semaines -> 5 jours (IaC + identite federee)

✓ Zero vendor lock-in : migration workloads batch AWS -> GCP demontree en 2 semaines

## Conclusion

Le multi-cloud est une realite pour la plupart des PME en croissance. La vraie question n'est pas 'est-ce que je veux etre multi-cloud' — c'est souvent deja le cas. La question est 'est-ce que je le gere de maniere intentionnelle ou j'accumule de la dette operationnelle ?'

Regle BOTUM : commencez par l'inventaire, definissez le role de chaque cloud, federez les identites, puis ajoutez les couches d'abstraction. Dans cet ordre.