

Guide Cloud Hybride

Architecture équilibrée pour PME canadienne

PIPEDA/Loi 25 · Azure Arc · VPN · Cas concret -35% coûts

On-Prem + **Cloud Public** = **Architecture Hybride**

Mars 2026

Cloud Hybride : l'architecture équilibrée pour PME canadienne

Le terme "cloud hybride" est partout. Derrière le buzzword : des workloads qui tournent à la fois sur votre infrastructure on-premises et sur un cloud public, orchestrés ensemble via une couche de gestion unifiée. Pas deux mondes séparés — un seul système cohérent.

Pourquoi les PME canadiennes choisissent le modèle hybride

1. LPRPDE et Loi 25 (Québec) — Contraintes sur la résidence des données canadiennes. Garder certaines données on-prem ou en régions certifiées (Azure Canada Central) n'est pas de la paranoïa — c'est de la conformité.
2. Latence des applications critiques — ERP, bases de données de production, systèmes temps-réel : ces workloads n'ont rien à gagner dans le cloud. La latence réseau ajoute 5-20ms.
3. Coûts réels vs estimés — L'egress coûte. Le stockage objet à haute fréquence coûte. Garder les données froides on-prem et utiliser le cloud pour le compute variable : c'est là que les économies deviennent réelles.
4. Applications legacy non migrables — SQL Server 2008, AS/400, CAO bare-metal. Le cloud hybride permet de les maintenir sans bloquer l'organisation.

Les 3 Patterns Hybrides

Extend — Burst to Cloud

Infra on-prem gère la charge de base. Le cloud absorbe les pics. Typique pour l'e-commerce saisonnier, batch nocturne, dev/test. Vous payez le cloud uniquement quand vous en avez besoin. Outils : Azure Autoscale, AWS Auto Scaling.

Bridge — DR/Backup

On-prem reste primaire. Le cloud = plan B : DR, backup géo-redondant, réplication continue. RTO de 4h → 45 minutes. Coût mensuel : 300-800\$ pour une PME 100 serveurs. Outils : Azure Site Recovery, AWS Backup.

Full Hybrid — Workloads distribués

Chaque workload placé selon son profil. Données PII → on-prem. Compute ML intensif → cloud. SaaS pour la collaboration. Le plus rentable à maturité. Outils : Azure Arc, AWS Outposts, GCP Anthos.

Stack technique recommandée : Azure Arc, AWS Outposts, GCP Anthos

Plateforme	Modèle	Forces	Idéal pour	Coût
------------	--------	--------	------------	------

Azure Arc	Agent léger sur vos serveurs	Azure Policy, Defender, Monitor Linux/Win/K8s	Stack Microsoft existante	0\$ base + services attachés
AWS Outposts	Rack physique AWS dans votre DC	Latence ultra-faible Services AWS on-prem natifs	Besoin AWS API on-prem	10k-30k\$/mois (rack dédié)
GCP Anthos	Kubernetes géré multi-cloud	GKE partout Istio intégré Multi-cloud natif	Kubernetes-first multi-cloud	0.10\$/vCPU-h + infra

Recommandation PME canadienne : Azure Arc pour les stacks Microsoft existantes (M365, Azure AD). Coût d'entrée minimal, gestion unifiée sans hardware supplémentaire.

Réseau hybride : VPN vs ExpressRoute vs Direct Connect

Option	Bande passante	Latence	Coût/mois	Quand utiliser
VPN site-à-site	1-10 Gbps	+10-30ms	30-150\$	<500 Mbps, budget serré
Azure ExpressRoute	1-100 Gbps	2-10ms	500-3000\$	>1 Gbps, critique latence
AWS Direct Connect	1-100 Gbps	2-10ms	500-3000\$	>1 Gbps, critique latence

Règle pratique : VPN pour démarrer et DR/backup. ExpressRoute/Direct Connect quand votre facture de bande passante dépasse 200\$/mois ou que vos apps réclament <5ms. Point de croisement : ~500 Mbps de trafic moyen quotidien.

Sécurité hybride : identité unifiée et zero trust

1. Identité unifiée

Azure AD/Entra ID (stack Microsoft) ou Okta (multi-cloud) comme Identity Provider central. SSO pour toutes les apps, MFA obligatoire, Conditional Access basé sur le risque.

2. Segmentation réseau

Micro-segmentation : chaque workload dans son propre sous-réseau, NSG/Security Groups stricts. Le trafic est-ouest (entre workloads) doit aussi être inspecté.

3. Zero Trust appliqué

Just-In-Time access pour les admins (Azure PIM), secrets dans Key Vault, logs centralisés dans SIEM (Sentinel). Minimum viable : MFA + Conditional Access + audit des accès privilégiés.

Erreurs communes à éviter

- Tout migrer d'un coup — Approche : pilot 2-3 workloads non-critiques, mesurer, ajuster, puis scaler.
- Ignorer la latence des données — Règle : apps et données dans le même domaine (cloud ensemble, ou on-prem ensemble).
- Sous-estimer le réseau — Budget réseau minimum : 15-20% du budget cloud total.
- Oublier la gouvernance des coûts — Azure Cost Management dès le jour 1, alertes à 80% du budget.

Cas concret BOTUM : PME 150 employés, –35% de coûts

Client industriel, 150 employés, Montréal. 40 VMs sur-provisionnées dans Azure, facture : 18 000 \$/mois.

Stack hybride déployée :

- 12 VMs rapatriées on-prem (ERP, SQL production, MES) → Proxmox local
- Azure Arc sur les serveurs Proxmox : gestion unifiée, Azure Policy, Defender
- VPN site-à-site : Fortinet on-prem + Azure VPN Gateway (Active-Active)
- Azure maintenu : Azure AD, M365, AKS pour apps web, stockage objet froid
- DR : Azure Site Recovery pour VMs critiques (RTO 45 min)

Résultats après 6 mois :

Métrique	Avant	Après (hybride)
Facture Azure mensuelle	18 000 \$/mois	11 700 \$/mois (–35%)
Latence ERP	55ms	3ms
Conformité PIPEDA	Partielle	100% (données on-prem)
RTO Disaster Recovery	4 heures	45 minutes
Visibilité infra unifiée	Aucune	Azure Arc Dashboard

□ Aller plus loin avec BOTUM

Architecture cloud hybride, migration, sécurité — les équipes BOTUM accompagnent les PME canadiennes.

→ Discuter de votre projet : www.botum.ca/contact

Partagez ce guide avec votre équipe.

↓ www.botum.ca/guides/guide-cloud-hybride-architecture-pme-fr.pdf