



Veille Technologique Quotidienne

Technique

25 septembre 2026 – Fréquence : Quotidienne (du Lundi au Vendredi)

Synthèse & Sujet du Jour

OpenShift Service Mesh 3 & Istio Ambient Mode : Architecture Sidecarless, ztunnel L4 et Waypoint Proxies L7

Découvrez l'architecture sans sidecar d'OpenShift Service Mesh 3 : chiffrement mTLS L4 transparent via ztunnel Rust, proxies Waypoint L7 à la demande et réduction drastique de l'overhead mémoire.

1. Périmètre

Famille de veille : 2. Métiers, Compétences & Technologies.

Fréquence d'exécution : Quotidienne (du Lundi au Vendredi à 08h30).

Diffusion : [Radar Web Aperta](#) — [LinkedIn Aperta Scientia](#) — [X @ApertaScientia](#).

2. Sujet du Jour — Article Publié sur le Radar Web

OpenShift Service Mesh 3 & Istio Ambient Mode : Architecture Sidecarless, ztunnel L4 et Waypoint Proxies L7

L'adoption historique des maillages de services (*service meshes*) s'est longtemps heurtée à une contrainte opérationnelle majeure : l'injection systématique d'un conteneur sidecar Envoy dans chaque Pod applicatif. Cette approche traditionnelle générait une surconsommation de mémoire VRAM/RAM, des complexités de cycle de vie (séquençement d'initialisation, terminaison des jobs éphémères) et imposait un redémarrage complet de tous les pods lors des montées de version du mesh.

Avec **OpenShift Service Mesh 3** (fondé sur **Istio Ambient Mode**), l'architecture réseau franchit un cap décisif grâce au paradigme *sidecarless*.

1. Séparation des couches et mTLS transparent via ztunnel (L4)

Le modèle Ambient découple strictement le transport sécurisé L4 des fonctionnalités applicatives L7 :

- **DaemonSet ztunnel ultra-léger** : Déployé par nœud et écrit en Rust, le *Zero Trust Tunnel* (ztunnel) intercepte le trafic local au niveau du sous-système réseau du noyau Linux sans modifier les manifestes applicatifs.
- **Protocole HBONE (HTTP-Based Overlay Network)** : Le chiffrement mutuel mTLS et l'authentification cryptographique SPIFFE/SPIRE sont établis nativement et de manière transparente entre nœuds via des tunnels encapsulés L4 (port 15008).
- **Zéro redémarrage applicatif** : L'activation du chiffrement Zero-Trust sur un namespace s'effectue par simple



étiquetage (`istio.io/dataplane-mode=ambient`), sans aucune interruption des charges de travail en production.

2. Proxies Waypoint déclaratifs à la demande (L7)

Le traitement applicatif avancé de couche 7 n'est plus imposé partout :

- **Isolation ciblée** : Les proxies Envoy L7 (nommés *Waypoint*) ne sont instanciés que pour les services nécessitant des règles avancées : routage fin, injection de fautes, analyse HTTP/gRPC, rate limiting ou politiques d'autorisation RBAC granulaires.
- **Périmètre personnalisable** : Un proxy Waypoint peut être partagé à l'échelle d'un namespace ou dédié à un `ServiceAccount` spécifique, simplifiant la maintenance et la gestion des accès sans compromettre la sécurité.

3. Réduction drastique de l'empreinte & compatibilité IA / MLOps

L'architecture sans sidecar élimine les frictions majeures sur les clusters hybrides :

- **Économie de ressources massive** : Suppression de l'allocation mémoire fixe de 50 à 100 Mo par Pod, libérant des dizaines de gigaoctets sur les clusters à forte densité de microservices.
- **Fluidité pour les pipelines IA & Jobs MLOps** : Les tâches éphémères (Kubeflow Pipelines, Ray Jobs, workers PyTorch) et les gros ServingRuntimes (vLLM, KServe) ne souffrent plus de blocages à la fermeture liés à l'attente du conteneur sidecar.

4. Compétences & Cursus Aperta Scientia

- **Cursus AS200 (DevOps Platform Engineer — 399h)** : Maîtrise des architectures réseau Cloud-Native, sécurité Zero-Trust avec OpenShift Service Mesh 3 et intégration GitOps (modules **DO380** et **DO280**).
- **Cursus AS300 (AI Platform Engineer — 399h)** : Sécurisation et observabilité des flux d'inférence distribuée multi-modèles sans dégradation de la latence réseau.

5. Sources & Références Techniques

- **Istio Ambient Mode Architecture** : [__HREF_0__](#)
- **Red Hat OpenShift Service Mesh Documentation** : [__HREF_0__](#)
- **CNCF Istio Project** : [__HREF_0__](#)

3. Impact sur les Cursus Aperta Scientia

Cursus AS200 — DevOps Platform Engineer

Cette veille alimente directement les modules d'ingénierie de plateforme et de sécurisation avancée de la chaîne de livraison logicielle :



- **Construction & CI/CD (D0288)** : Conception de pipelines déclaratifs Tekton, gestion des builds conteneurisés en environnement sans privilèges (*rootless*) et automatisation via Pipelines-as-Code.
- **Exploitation & Durcissement (D0380)** : Gestion multi-cluster, observabilité de la chaîne de livraison et politiques de conformité à l'échelle.
- **Sécurisation Conteneurs & Plateforme (D0430)** : Implémentation du contrôle d'admission (Sigstore Policy Controller, RHACS), signature keyless d'artefacts (RHTAS), génération de SBOM et analyse continue d'exploitabilité (TPA / VEX).
- **Certifications préparées** : Préparation opérationnelle aux examens **EX188** (Containers), **EX280** (OpenShift Administration) et **EX288** (OpenShift Development).

Cursus AS300 — AI Platform Engineer

La démarche de sécurisation de la supply chain logicielle est transposée à l'infrastructure d'inférence et aux pipelines MLOps :

- **Traçabilité des dépendances GPU & ML** : Audit de provenance et validation SLSA des images de base contenant les runtimes CUDA, ROCm et PyTorch.
- **Signature & Contrôle des Modèles** : Signature cryptographique des poids de modèles et des runtimes de serving vLLM / KServe avant déploiement en cluster.
- **Gouvernance & SBOM IA** : Inventaire automatisé des licences et détection proactive des vulnérabilités sur la pile MLOps (KubeFlow Pipelines, Ray, Triton).

4. Sources

- Red Hat Developer Blog — [Lien](#)
- OpenShift Documentation — [Lien](#)
- Kubernetes Community Documentation — [Lien](#)
- CNCF Cloud Native Landscape — [Lien](#)
- vLLM Project Documentation — [Lien](#)
- Sigstore Documentation — [Lien](#)
- SLSA Framework — [Lien](#)

Contacts & Communauté :

- Direction des Formations : learning@apertascientia.io
- Référent Handicap & Bien-être (Care) : care@apertascientia.io
- X (Twitter) : [@ApertaScientia](https://twitter.com/ApertaScientia)
- Communauté Discord : discord.gg/eDJzR5Vk85