+33 (0)1 48 10 09 46
formation@ambient-it.net
140 Avenue Jean Lolive 93500 Pantin - France

Mis à jour le 17/02/2026

S'inscrire

Formation Kiali

2 jours (14 heures)

Présentation

Kiali est la console d'observabilité d'Istio pour visualiser votre service mesh, diagnostiquer les flux et sécuriser les échanges. Elle aide à comprendre rapidement la topologie, détecter les erreurs et valider les politiques (mTLS, routage, RBAC) en conditions réelles.

Cette formation se concentre sur l'usage opérationnel de Kiali pour piloter un mesh Istio : lecture des graphes, analyse des métriques, inspection des configurations et investigation d'incidents (latence, 5xx, timeouts). Vous apprendrez à relier les symptômes observés dans Kiali aux ressources Istio (VirtualService, DestinationRule, Gateway) et à corriger sans tâtonner.

L'approche est pratique : démos guidées, ateliers de troubleshooting, scénarios de canary/traffic shifting et durcissement mTLS. Livrables : un environnement de lab reproductible, une checklist de diagnostic et des commandes/bonnes pratiques pour exploiter Kiali au quotidien.

Comme toutes nos formations, celle-ci vous présentera **la dernière version stable** de la technologie et ses nouveautés.

Objectifs

- Installer et configurer Kiali dans un cluster Kubernetes avec Istio.
- Interpréter le graphe de services et isoler les dépendances critiques.
- Diagnostiquer erreurs, latence et timeouts via métriques et traces.
- Valider et corriger le routage (canary, mirroring, retries, circuit breaking).
- Auditer la sécurité du mesh (mTLS, policies) et vérifier la conformité.

Public visé

- Ingénieurs DevOps / SRE
- Administrateurs Kubernetes
- Développeurs back-end en environnement microservices
- Architectes cloud

Pré-requis

- Bonnes bases de Kubernetes (pods, services, ingress, namespaces)
- Notions d'Istio (sidecar, gateways, VirtualService)
- Pratique du terminal et de kubectl
- Compréhension HTTP/gRPC et codes d'erreur

Pré-requis techniques

- PC avec 16 Go RAM recommandé (8 Go minimum)
- Linux, macOS ou Windows avec WSL2
- Outils : kubectl, istioctl, Helm, un éditeur de code
- Accès à un cluster Kubernetes (local type kind/minikube ou distant) avec droits admin

Programme de formation Kiali Istio

[Jour 1 - Matin]

Fondamentaux Istio et prise en main de Kiali

- Rappels Service Mesh : data plane, control plane, sidecar Envoy
- Composants Istio clés : istiod, injection, gateways, namespaces et labels
- Kiali : rôle, prérequis, accès, notions de Graph, Workloads, Services, Applications
- Lecture des métriques et dépendances : trafic, latence, erreurs, seuils et agrégations
- Atelier pratique : Déployer Istio + Kiali sur un cluster et valider l'injection sidecar.

[Jour 1 - Après-midi]

Observabilité du trafic et diagnostic avec Kiali

- Générer du trafic applicatif et interpréter le Service Graph (edges, rates, protocoles)
- Analyse des health checks Kiali : configuration, mTLS, Istio objects, warnings
- Corrélation avec Prometheus et Grafana : métriques utiles (p95, 4xx/5xx, saturation)
- Inspection des workloads : logs, ports, labels, versioning, pods et readiness
- Atelier pratique : Diagnostiquer une dégradation (latence/erreurs) à partir du graphe et des métriques.

[Jour 2 - Matin]

Gestion du trafic Istio (VirtualService, DestinationRule) via Kiali

- Objets de routage : Gateway, VirtualService, DestinationRule, subsets et versions
- Cas d’usage : canary, blue/green, mirroring, règles par headers/cookies
- Validation et linting Kiali : détection d’incohérences, conflits de routes, ports/protocoles
- Visualiser l’impact des règles : évolution du trafic par version dans le graphe
- Atelier pratique : Mettre en place un canary 90/10 puis basculer 100% en s’appuyant sur Kiali.

[Jour 2 - Après-midi]

Sécurité, mTLS et politiques : contrôle et vérification avec Kiali

- mTLS : modes PERMISSIVE/STRICT, PeerAuthentication et DestinationRule
- Autorisation : AuthorizationPolicy (principals, namespaces, paths, methods) et scénarios courants
- Détection des problèmes de sécurité dans Kiali : cadenas mTLS, warnings, objets manquants
- Bonnes pratiques d’exploitation : scopes par namespace, conventions de labels, audit des changements
- Atelier pratique : Activer mTLS STRICT et appliquer une AuthorizationPolicy, puis valider le résultat dans Kiali.

Sociétés concernées

Cette formation s’adresse à la fois aux particuliers ainsi qu’aux entreprises, petites ou grandes, souhaitant former ses équipes à une nouvelle technologie informatique avancée ou bien à acquérir des connaissances métiers spécifiques ou des méthodes modernes.

Positionnement à l'entrée en formation

Le positionnement à l'entrée en formation respecte les critères qualité Qualiopi. Dès son inscription définitive, l'apprenant reçoit un questionnaire d’auto-évaluation nous permettant d’apprécier son niveau estimé sur différents types de technologies, ses attentes et objectifs personnels quant à la formation à venir, dans les limites imposées par le format sélectionné. Ce questionnaire nous permet également d’anticiper certaines difficultés de connexion ou de sécurité interne en entreprise (intraentreprise ou classe virtuelle) qui pourraient être problématiques pour le suivi et le bon déroulement de la session de formation.

Méthodes pédagogiques

Stage Pratique : 60% Pratique, 40% Théorie. Support de la formation distribué au format numérique à tous les participants.

Organisation

Le cours alterne les apports théoriques du formateur soutenus par des exemples et des séances de réflexions, et de travail en groupe.

Validation

À la fin de la session, un questionnaire à choix multiples permet de vérifier l’acquisition correcte des compétences.

Sanction

Une attestation sera remise à chaque stagiaire qui aura suivi la totalité de la formation.

Organisme de formation enregistré sous le numéro 11 75 54743 75. Cet enregistrement ne vaut pas agrément de l’État.
© Ambient IT 2015-2026. Tous droits réservés. Paris, France - Suisse - Belgique - Luxembourg