

Formation Kong Gateway – Administration

Réf. SF34573

Maîtrisez la sécurisation, le dépannage et l'administration déclarative de Kong Gateway pour opérer une plateforme API fiable en environnement de production.

2 j Durée	1 700 € HT Inter / participant	4 200 € HT Intra (≤12 pers.)	0 Sessions à venir
--------------	-----------------------------------	---------------------------------	-----------------------

Objectifs pédagogiques

- ✓ Sécuriser le Control Plane de Kong Gateway en configurant le RBAC, les permissions workspaces et le hardening de Kong Manager et de l'Admin API
- ✓ Protéger le Data Plane en mettant en oeuvre le rate limiting, l'authentification JWT et le mutual TLS (mTLS)
- ✓ Intégrer un fournisseur d'identité externe via le plugin OpenID Connect (OIDC)
- ✓ Configurer et exploiter les plugins avancés de transformation de requêtes/réponses et de métriques Prometheus
- ✓ Diagnostiquer et résoudre les problèmes de production à l'aide d'une méthodologie de dépannage structurée
- ✓ Administrer Kong Gateway de manière déclarative avec deck (export, synchronisation, manifestes YAML)
- ✓ Planifier et exécuter une mise à jour de Kong Gateway en suivant les bonnes pratiques de migration

Public visé & prérequis

Public visé Administrateurs systèmes et réseaux, Ingénieurs DevOps

Prérequis- Avoir suivi la formation "Kong Gateway - Fondations" (ou connaissances équivalentes en concepts API Gateway, installation et configuration de base de Kong) - Connaissances Linux de base (navigation en ligne de commande, édition de fichiers de configuration) - Familiarité avec Docker et les environnements conteneurisés - Notions de réseau (DNS, TLS, certificats)

Programme détaillé

Déploiement et cycle de vie de Kong Gateway

- Options de déploiement en production : choix entre single node, cluster et conteneurs selon les exigences de disponibilité et de performance
- Dimensionnement d'une instance Kong : critères de sizing CPU, mémoire et connexions pour anticiper la charge réelle
- Tests de fumée post-installation : validation fonctionnelle pour confirmer la santé de la plateforme avant mise en service
- Modèle de versionnement Kong : comprendre la politique de versions pour planifier les montées de version
- Procédure de migration : exécution d'un rolling upgrade en minimisant l'impact sur le trafic
- Bonnes pratiques de mise à jour : stratégies de rollback et précautions spécifiques par version

Activités pratiques :

- Déploiement d'une instance Kong Gateway conteneurisée et exécution d'un plan de tests de fumée
- Simulation d'une migration de version avec vérification de la continuité de service

Sécurisation du Control Plane

- Authentification vs autorisation (AuthN/AuthZ) : distinguer les mécanismes de vérification d'identité et de gestion des droits
- RBAC (Role-Based Access Control) : création de rôles et attribution de permissions granulaires pour contrôler l'accès administrateur
- Sécurisation de Kong Manager : restriction de l'interface d'administration pour limiter la surface d'attaque
- Verrouillage de l'Admin API : protection de l'API d'administration par filtrage réseau, authentification et bonnes pratiques de hardening
- Permissions workspaces : isolation des environnements et délégation contrôlée entre équipes

Activités pratiques :

- Configuration du RBAC avec création de rôles différenciés (admin, lecture seule, opérateur)
- Sécurisation de l'accès à Kong Manager et test des restrictions d'accès

Sécurisation du Data Plane

- Rate limiting : configuration de la limitation de débit pour protéger les backends contre les pics de trafic et les abus
- Authentification JWT : mise en place de la vérification de tokens pour sécuriser l'accès aux API exposées
- Mutual TLS (mTLS) : chiffrement et authentification bilatérale des communications entre clients et gateway
- Hardening du Data Plane : renforcement global des paramètres de sécurité pour réduire la surface d'exposition
- Sécurisation des échanges inter-nœuds : protection des communications entre Control Plane et Data Plane en environnement distribué

Activités pratiques :

- Mise en place d'une politique de rate limiting sur une route de production
- Configuration d'une authentification JWT de bout en bout sur une API
- Activation du mTLS entre un client et Kong Gateway

Intégration OpenID Connect (OIDC)

- Protocole OIDC et fournisseurs d'identité : principes de la délégation d'authentification à un IdP externe
- Paramétrage du plugin OIDC Kong : configuration des endpoints, secrets et scopes pour connecter Kong à un Identity Provider
- Flux d'authentification : fonctionnement de l'Authorization Code Flow et de l'Implicit Flow selon les cas d'usage
- Administration et dépannage du plugin OIDC : gestion des sessions, renouvellement de tokens et diagnostic des erreurs courantes

Activités pratiques :

- Intégration de Kong Gateway avec un IdP (Keycloak ou équivalent) via le plugin OIDC
- Test d'un flux Authorization Code complet et vérification de l'accès conditionnel

Plugins avancés de transformation et de métriques

- Rate limiting avancé : stratégies de compteurs distribués et politiques de limitation multi-critères pour les architectures à grande échelle
- Transformation de requêtes et réponses : enrichissement, filtrage et réécriture des headers et body à la volée
- Plugin jq : manipulation JSON avancée pour transformer dynamiquement les payloads sans code custom
- Plugin exit transformer : personnalisation des réponses d'erreur pour harmoniser le format des messages renvoyés aux consommateurs
- Plugin Prometheus : exposition des métriques de performance et de trafic pour alimenter une stack de monitoring

Activités pratiques :

- Configuration de transformations de requêtes/réponses sur une route existante
- Activation du plugin Prometheus et consultation des métriques exposées

Dépannage et diagnostic en production

- Méthodologie de troubleshooting structurée : approche systématique pour isoler et résoudre les incidents Kong Gateway
- Problèmes upstream vs downstream : distinction entre les erreurs côté backend et côté client pour orienter le diagnostic
- Collecte d'informations diagnostiques : exploitation des logs, métriques et codes de statut pour accélérer la résolution
- Problèmes courants en production : identification rapide des erreurs de configuration, de réseau et de sécurité les plus fréquentes

Activités pratiques :

- Résolution d'incidents simulés sur des scénarios réalistes de production (erreur de routage, certificat expiré, plugin mal configuré)
- Analyse de logs Kong et corrélation avec les métriques pour diagnostiquer un problème de performance

Administration déclarative avec deck

- Configuration déclarative vs impérative : avantages de l'approche Infrastructure as Code pour la gestion de Kong Gateway
- CLI deck : maîtrise des commandes dump, sync, diff et ping pour piloter la configuration depuis le terminal
- Manifestes YAML : structure, conventions et bonnes pratiques pour rédiger des fichiers de configuration maintenables
- Synchronisation d'environnements : propagation contrôlée de la configuration entre développement, staging et production
- Ouverture CI/CD : positionnement de deck dans un pipeline d'intégration continue pour automatiser les déploiements de configuration

Activités pratiques :

- Export de la configuration courante avec deck et comparaison avec un état cible via diff
- Modification d'un manifeste YAML et synchronisation vers un environnement Kong Gateway

– Simulation d'un workflow de promotion de configuration entre deux environnements

Pourquoi choisir Sparks Formation ?

20 ans d'expertise IT, des formateurs experts et des sessions garanties contre l'annulation.

20 ans
d'expertise

1 068+
formations

11 178
apprenants formés/an

+67
Net Promoter Score

Avis des participants

Note moyenne des participants de la filière Développement et Ingénierie de Logiciels : 4,9/5 — 165 avis

Donatien W. — Formation dense mais très digeste avec beaucoup de points abordés. Les spécificités de chacun ont pu être abordées.

Jean-Baptiste M. — Le format 3 jours est une contrainte forte. A la sortie de cette formation, on attaque à peine la "vallée du doute" et on sent qu'il y a...

Ils nous font confiance

Cette année notre filière Architecture & Design Logiciel a accompagné plus de 50 entreprises dont :

SOPRA STERIA CIMPA SAS THALES GLOBAL SERVICES SAS ADEO SERVICES AUBAY LBC FRANCE ORANGE BUSINESS Sqli WORLDLINE FRANCE SAS ADEVINTA +40 autres

Financement & certifications

Cette formation est éligible aux financements OPCO et FNE-Formation. Nos équipes vous accompagnent dans le montage de votre dossier.



Réservez votre place dès maintenant

20 ans d'expertise · 1 000+ formations · NPS +67 · réponse sous 24h ouvrées

0 805 950 800

demande@sparks-formation.com