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

Mis à jour le 05/06/2026

S'inscrire

Formation OpenBao

4 jours (28 heures)

Présentation

OpenBao est une solution open source de gestion des secrets pour les entreprises. Cette plateforme permet de stocker, distribuer et contrôler l'accès aux secrets, aux certificats et aux clés cryptographiques utilisés par les applications modernes.

Notre formation OpenBao vous permettra de maîtriser l'installation, la configuration et l'exploitation d'un coffre-fort de secrets dans un contexte DevSecOps. Vous serez en mesure de créer des policies, d'activer des méthodes d'authentification, de gérer des tokens et de sécuriser les accès applicatifs.

Mais aussi de configurer les moteurs KV, les secrets dynamiques, la rotation automatique et l'intégration avec Kubernetes. OpenBao permet de centraliser la gouvernance des secrets tout en réduisant les risques liés aux credentials statiques.

De plus, OpenBao s'intègre aux environnements cloud native, aux pipelines CI/CD et aux architectures haute disponibilité.

À la suite de cette formation, vous serez en mesure d'installer, administrer et superviser OpenBao ainsi que de comprendre son architecture.

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

Objectifs

- Comprendre l'architecture et les composants d'OpenBao
- Installer, configurer et sécuriser un serveur OpenBao
- Gérer les tokens, policies et méthodes d'authentification

- Administrer les moteurs de secrets statiques et dynamiques
- Intégrer OpenBao avec Kubernetes et les pipelines CI/CD
- Déployer OpenBao en haute disponibilité et appliquer les bonnes pratiques de gouvernance

Public visé

- Administrateurs systèmes et cloud
- Ingénieurs DevOps, SRE et plateformes
- Ingénieurs sécurité et DevSecOps
- Architectes techniques et cloud native
- Développeurs amenés à consommer des secrets applicatifs

Pré-requis

- Connaissances de base en administration Linux
- Notions de sécurité applicative et de gestion des accès
- Compréhension générale des architectures cloud ou DevOps
- Des bases Kubernetes sont un plus pour les modules d’intégration

Pré-requis techniques

- Disposer d’un ordinateur avec un système Linux, macOS ou Windows avec WSL2
- Installer un terminal compatible et un éditeur de code, par exemple Visual Studio Code
- Installer Docker pour les environnements de démonstration et les ateliers pratiques
- Installer kubectl et disposer d’un cluster Kubernetes local ou distant pour les modules Kubernetes
- Prévoir une connexion Internet stable pour télécharger les images, dépendances et outils nécessaires

Formation OpenBao

[Jour 1 - Matin]

Fondamentaux de la gestion des secrets

- Comprendre le rôle d’OpenBao dans une architecture DevSecOps
- Identifier les enjeux liés aux secrets, aux tokens, aux certificats et aux clés applicatives
- Découvrir le positionnement d’OpenBao comme solution open source de secrets management
- Comparer les pratiques classiques de stockage avec l’usage d’un coffre-fort de secrets
- Comprendre les notions de seal, unseal, root token, policy et secret engine
- Atelier pratique : installer OpenBao, initialiser le serveur et manipuler les premières commandes CLI

[Jour 1 - Après-midi]

Architecture et configuration serveur

- Comprendre l’architecture d’un serveur OpenBao et ses composants principaux
- Configurer les listeners, le stockage, les paramètres TLS et les variables d’environnement
- Étudier le fonctionnement du chiffrement des données au repos
- Découvrir les backends de stockage : fichier, Raft, Consul et solutions compatibles
- Analyser les logs, le statut serveur et les premières commandes d’administration
- Mettre en place une configuration locale propre pour les exercices suivants

Moteur KV et structuration des secrets

- Activer et configurer le moteur KV secrets engine
- Comparer KV v1 et KV v2 : versioning, rollback, soft delete et destroy
- Organiser les chemins de secrets par application, équipe et environnement
- Définir des conventions de nommage exploitables en production
- Manipuler les opérations courantes : lecture, écriture, suppression et restauration
- Atelier pratique : créer une arborescence de secrets versionnés pour plusieurs environnements

[Jour 2 - Matin]

Policies, tokens et modèle d’autorisation

- Comprendre le modèle d’autorisation basé sur les policies
- Créer des policies adaptées aux applications, équipes et environnements
- Gérer les tokens, durées de vie, renouvellements, révocations et permissions
- Appliquer le principe du moindre privilège dans l’accès aux secrets
- Tester et déboguer les erreurs de permissions avec le CLI et l’API
- Atelier pratique : écrire des policies précises et valider les droits d’accès avec différents tokens

[Jour 2 - Après-midi]

Méthodes d’authentification applicative

- Découvrir les méthodes d’authentification disponibles dans OpenBao
- Configurer l’authentification userpass pour les usages d’apprentissage et d’administration
- Mettre en place AppRole pour les applications et services automatisés
- Comprendre les notions de RoleID, SecretID, TTL et usage limité
- Sécuriser l’authentification applicative dans un contexte CI/CD ou serveur
- Atelier pratique : connecter une application de test à OpenBao avec AppRole.

Secrets dynamiques et rotation

- Comprendre la différence entre secrets statiques et secrets dynamiques
- Découvrir les usages avec bases de données, comptes temporaires et accès applicatifs
- Configurer les notions de TTL, lease, renouvellement et révocation
- Mettre en place une stratégie de rotation des secrets
- Identifier les bénéfices sécurité : réduction de l'exposition, traçabilité et révocation rapide
- Atelier pratique : générer des credentials temporaires et tester leur expiration.

[Jour 3 - Matin]

Intégration Kubernetes

- Comprendre les limites des Secrets Kubernetes natifs
- Configurer l'authentification Kubernetes avec les service accounts
- Associer les workloads Kubernetes à des policies OpenBao dédiées
- Étudier les patterns d'intégration : init container, sidecar, injection et CSI driver
- Sécuriser l'accès aux secrets pour des applications cloud native
- Atelier pratique : authentifier un workload Kubernetes et récupérer un secret depuis OpenBao.

[Jour 3 - Après-midi]

Intégration applicative et API

- Utiliser le CLI, l'API HTTP et les clients applicatifs
- Consommer des secrets depuis des applications Node.js, Python, Go ou Java
- Gérer les erreurs courantes : token expiré, accès refusé, chemin incorrect, secret détruit
- Mettre en place des stratégies de cache applicatif et de renouvellement sécurisé
- Éviter les anti-patterns : secrets en logs, tokens persistants, droits trop larges
- Structurer une intégration propre entre OpenBao et les applications métier

CI/CD et automatisation DevSecOps

- Intégrer OpenBao dans une chaîne CI/CD
- Récupérer des secrets de manière sécurisée dans GitLab CI, GitHub Actions ou Jenkins
- Automatiser la configuration avec scripts, API et principes d'Infrastructure as Code
- Gérer les environnements développement, recette, staging et production

- Mettre en place des garde-fous contre l’exposition de secrets dans les dépôts Git
- Atelier pratique : connecter une pipeline CI/CD à OpenBao pour récupérer un secret temporaire.

[Jour 4 - Matin]

Haute disponibilité et exploitation

- Comprendre les enjeux de haute disponibilité pour un coffre-fort de secrets
- Déployer OpenBao avec le stockage intégré Raft
- Comprendre les rôles des nœuds, le quorum, le leader et les mécanismes de reprise
- Gérer les opérations de sauvegarde, restauration et redémarrage sécurisé
- Superviser le statut du cluster, les logs et les métriques essentielles
- Atelier pratique : déployer un cluster OpenBao simplifié et simuler une panne de nœud.

[Jour 4 - Après-midi]

Sécurité, audit et durcissement

- Activer et exploiter les audit devices
- Analyser les accès, les erreurs, les tokens et les opérations sensibles
- Appliquer les bonnes pratiques de hardening : TLS, policies minimales, rotation et séparation des rôles
- Mettre en place des alertes sur les comportements anormaux
- Définir une stratégie de revue périodique des accès et des secrets
- Préparer une checklist sécurité avant mise en production

Gouvernance, migration et cas final

- Définir une stratégie de gouvernance des secrets à l’échelle de l’organisation
- Préparer une migration depuis Vault ou une solution existante de secrets management
- Construire un runbook d’exploitation : incident, compromission, rotation d’urgence et restauration
- Définir les responsabilités entre équipes sécurité, DevOps, SRE et développement
- Élaborer une trajectoire d’adoption progressive d’OpenBao en production
- Atelier pratique : réaliser un cas fil rouge complet combinant policies, secrets, AppRole, audit et remédiation.

Pour aller plus loin

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.