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

Mis à jour le 11/08/2026

S'inscrire

Formation Certification Kubernetes Network Engineer (CKNE)

4 jours (28 heures)

Présentation

La formation Certification Kubernetes Network Engineer (CKNE) vous prépare à valider des compétences clés en réseau Kubernetes,CNI,DNS,politiques réseau et observabilité. Pensée pour l'examen officiel, elle vous aide à consolider une expertise opérationnelle et directement mobilisable en production.

Avec cette formation, vous apprendrez à structurer une compréhension solide des flux réseau dans Kubernetes, à diagnostiquer les problématiques de connectivité et à maîtriser les mécanismes qui conditionnent la fiabilité des applications conteneurisées.

Vous verrez comment exploiter les composants essentiels du réseau de cluster, depuis l'intégration des plugins CNI jusqu'à la gestion du trafic, des services, du DNS, des politiques de sécurité et des outils de dépannage avancés.

La préparation met également l'accent sur les compétences attendues pour l'examen CKNE, avec des mises en situation, des cas de configuration et des exercices de validation des acquis pour renforcer votre autonomie.

À l'issue de la formation, vous serez en mesure d'analyser une architecture réseau Kubernetes, de résoudre des incidents courants, de sécuriser les échanges et de vous présenter à la certification avec une préparation structurée et ciblée.

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

Objectifs

- Comprendre l'architecture réseau Kubernetes et les principaux flux entre pods, services et nœuds.
- Maîtriser les notions de CNI, d'IPAM, de DNS et de routage dans un cluster.
- Savoir diagnostiquer les problèmes de connectivité, de résolution de noms et de trafic inter-services.
- Appliquer les bonnes pratiques de sécurisation réseau avec les Network Policies et le chiffrement.
- Préparer efficacement l'examen CKNE à partir de scénarios proches des attentes de certification.

Public visé

- Ingénieur DevOps
- Administrateur Kubernetes
- Ingénieur réseau
- Architecte cloud
- Ingénieur plateforme

Pré-requis

- Connaissances de base en Kubernetes et en orchestration de conteneurs.
- Maîtrise des fondamentaux Linux, réseau IP et ligne de commande.
- Pratique des environnements Docker ou d'autres technologies de conteneurisation.
- Compréhension des concepts de TCP/IP, de routage et de résolution DNS.
- Expérience préalable en administration système, exploitation cloud ou DevOps.

Pré-requis techniques

- Un ordinateur récent avec navigateur à jour et une configuration suffisamment confortable pour les labs.
- Une connexion Wi-Fi ou Ethernet stable pour suivre les démonstrations et exercices en ligne.
- Un terminal fonctionnel avec kubectl installé pour les manipulations Kubernetes.
- Un environnement de travail avec Docker ou un accès à un cluster de test si demandé par le formateur.
- En classe virtuelle, un micro et un casque pour participer aux échanges et aux ateliers.

Programme de notre formation Kubernetes Network Engineer (CKNE)

[Jour 1 - Matin]

Fondamentaux du réseau Kubernetes

- Rappel des objectifs de la certification CKNE et du périmètre évalué.
- Architecture réseau d'un cluster, rôles des nœuds, des pods et des services.
- Modèle de connectivité pod-to-pod et circulation du trafic dans le plan de données.
- Notions de CNI, d'overlay, de routage et d'IPAM.

- Lecture des schémas réseau pour identifier les points de rupture probables.
- Atelier pratique : cartographier le chemin d'un paquet entre deux pods et repérer les composants impliqués.

[Jour 1 - Après-midi]

Installation et configuration CNI

- Rôle des plugins CNI dans l'initialisation réseau des pods.
- Paramètres essentiels d'un plugin, interfaces, adressage et politiques associées.
- Gestion des plages Pod CIDR et cohérence avec le plan d'adressage du cluster.
- Impact des choix d'implémentation sur la latence, la maintenabilité et le dépannage.
- Bonnes pratiques pour vérifier l'état d'un plugin et isoler un défaut de configuration.
- Atelier pratique : installer et valider un plugin CNI dans un environnement de test.

[Jour 2 - Matin]

Services, kube-proxy et DNS

- Fonctionnement des Services Kubernetes et des types de service les plus courants.
- Rôle de kube-proxy dans l'acheminement du trafic vers les endpoints.
- Résolution de noms avec CoreDNS et dépendances entre service discovery et connectivité.
- Diagnostic des erreurs fréquentes, timeouts, endpoints absents, résolution DNS défaillante.
- Comparaison des mécanismes de publication interne et d'exposition du trafic.
- Atelier pratique : analyser un service défaillant et corriger la chaîne de résolution et de routage.

[Jour 2 - Après-midi]

Dépannage réseau avancé

- Méthode de diagnostic structurée pour les problèmes de connectivité dans Kubernetes.
- Utilisation de ip, tcpdump et iptables pour l'analyse paquet par paquet.
- Vérification des interfaces, des routes, des règles de filtrage et des tables de translation.
- Analyse des symptômes courants, perte de trafic, mauvaise MTU, DNS intermittent, endpoints injoignables.
- Construction d'un raisonnement de dépannage adapté aux questions de certification.
- Atelier pratique : résoudre un incident de connectivité en suivant une procédure de diagnostic pas à pas.

[Jour 3 - Matin]

Traffic management et exposition

- Principes de gestion du trafic dans et hors du cluster.
- Exposition des applications, chemins d'entrée, sortie et équilibrage de charge.
- Contrôle du trafic avec les Gateway API et les routes associées.
- Gestion des flux egress et des stratégies de sortie de cluster.
- Critères de choix entre plusieurs approches selon le besoin applicatif.
- Atelier pratique : configurer une exposition de service et vérifier le parcours des requêtes.

[Jour 3 - Après-midi]

Sécurité réseau et politiques

- Fondamentaux de la segmentation réseau dans Kubernetes.
- Création et lecture des Network Policies pour contrôler les accès.
- Gestion des communications autorisées entre namespaces, pods et services.
- Introduction au chiffrement des flux, aux certificats et aux protections au niveau transport.
- Approche sécurisée des communications sensibles et des surfaces d'attaque courantes.
- Atelier pratique : écrire et tester une politique réseau limitant les échanges entre workloads.

[Jour 4 - Matin]

Observabilité et supervision réseau

- Lecture des indicateurs utiles pour suivre la santé réseau d'un cluster.
- Utilisation des metrics pour détecter saturation, erreurs et anomalies de trafic.
- Apports des logs et du tracing pour reconstituer un incident de bout en bout.
- Corrélation entre symptômes applicatifs et causes réseau.
- Préparation aux questions de supervision et de diagnostic de l'examen CKNE.
- Atelier pratique : interpréter des métriques et traces pour identifier l'origine d'une dégradation réseau.

[Jour 4 - Après-midi]

Révision certifiante et mise en situation

- Revue structurée des domaines de la certification CKNE.
- Questions types et pièges fréquents rencontrés lors de la préparation.
- Méthode de lecture rapide d'un énoncé et d'élimination des distracteurs.
- Stratégie de révision ciblée sur les notions à fort poids dans l'examen.
- Bilan des acquis et plan d'entraînement individuel avant le passage officiel.
- Atelier pratique : réaliser une mini-simulation d'examen avec correction commentée.

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.