

Mis à jour le 26/10/2026

S'inscrire

Formation Cloud Custodian : adopter une démarche FinOps

3 jours (21 heures)

Présentation

Cloud Custodian est un moteur de règles permettant de gouverner les ressources cloud et d'automatiser leur optimisation. Avec ses politiques en YAML et ses mécanismes de filtrage, il accompagne une démarche FinOps fondée sur la maîtrise des usages, la responsabilisation des équipes et la réduction des dépenses inutiles.

Notre formation Cloud Custodian : adopter une démarche FinOps vous permettra de traduire vos objectifs économiques en politiques automatisées et contrôlées, à partir de cas concrets sur AWS.

Vous apprendrez à structurer vos règles, à contrôler le tagging des ressources, à identifier les usages sous-exploités et à programmer des arrêts hors des heures ouvrées. Vous mettrez également en place des notifications et des actions différées.

À l'issue de la formation, vous serez en mesure de déployer une gouvernance des coûts progressive, de sécuriser les remédiations et de distinguer les économies estimées des gains réellement observés dans les données de facturation.

Cette formation aborde également les tests des politiques et leur déploiement, la supervision des exécutions et les indicateurs de suivi afin d'inscrire vos optimisations dans une dynamique d'amélioration continue.

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

Objectifs

- Structurer une démarche FinOps articulant visibilité, optimisation et exploitation
- Concevoir et valider des politiques Cloud Custodian adaptées aux ressources cloud
- Détecter les défauts de tagging et les ressources potentiellement sous-utilisées
- Automatiser des optimisations avec des garde-fous opérationnels et des notifications
- Déployer les politiques et mesurer leurs effets sur les usages et les coûts

Public visé

- Ingénieur FinOps
- Ingénieur Cloud
- Ingénieur DevOps
- Architecte Cloud
- Administrateur Cloud

Pré-requis

- Expérience des ressources de calcul et de stockage sur AWS dans un environnement professionnel ou de laboratoire
- Connaissance des permissions et des rôles AWS IAM utilisés pour accéder aux ressources
- Maîtrise des commandes courantes dans un terminal et des fichiers YAML de configuration
- Notions de facturation cloud, de tagging et de suivi des consommations

Pré-requis techniques

- Ordinateur avec 8 Go de mémoire vive recommandés et un environnement Linux local ou virtualisé
- Installation de Python 3 dans une version maintenue et compatible avec la version de Cloud Custodian retenue pour les ateliers
- Installation de AWS CLI 2 et de Git avec un éditeur tel que Visual Studio Code pour modifier les politiques
- Accès à un compte AWS de laboratoire avec ressources dédiées, permissions adaptées et budget encadré
- Connexion Internet stable autorisant les téléchargements de dépendances et les accès aux API cloud nécessaires aux ateliers

Programme de notre formation Cloud Custodian : adopter une démarche FinOps

[Jour 1 - Matin]

Relier la démarche FinOps aux politiques cloud

- Les phases Inform, Optimize et Operate du cadre de la FinOps Foundation et la collaboration entre finance, métiers et équipes techniques

- Les leviers de réduction des coûts : optimisation des usages, tarification et limites du périmètre de Cloud Custodian
- Le fonctionnement de Cloud Custodian : ressources, filtres, actions et différences entre fournisseurs cloud
- La préparation du laboratoire AWS : environnement Python isolé, authentification et permissions minimales
- La structure d'une politique YAML, la découverte du schéma et la validation avec custodian validate
- Atelier pratique : Installer Cloud Custodian et exécuter en lecture seule une première politique d'inventaire sur les ressources du laboratoire.

[Jour 1 - Après-midi]

Fiabiliser le tagging et la visibilité des usages

- La définition d'une convention de tags FinOps : propriétaire, application, environnement et centre de coûts
- Les filtres value, les conditions sur les tags et les combinaisons logiques pour cibler les ressources
- La détection des tags absents ou non conformes et la gestion des exceptions
- La simulation avec --dryrun et l'analyse des ressources sélectionnées dans les fichiers de sortie
- Le rapprochement des inventaires avec les données de coûts et les conditions d'utilisation des tags pour l'allocation financière
- Atelier pratique : Construire une politique de contrôle des tags, analyser les écarts et produire un inventaire exploitable par propriétaire.

[Jour 2 - Matin]

Détecter et prioriser les opportunités d'optimisation

- L'identification des volumes EBS non attachés et des ressources candidates au nettoyage
- L'utilisation des filtres metrics et des métriques CloudWatch pour repérer les instances potentiellement sous-utilisées
- Le choix des seuils, des périodes d'observation et du traitement des données manquantes
- La distinction entre signal de sous-utilisation, recommandation de redimensionnement et décision validée par le propriétaire
- La priorisation selon les économies potentielles, les dépendances applicatives et le risque opérationnel
- Atelier pratique : Détecter des volumes inutilisés et des instances candidates à une optimisation, puis constituer un backlog chiffré à partir des données tarifaires fournies.

[Jour 2 - Après-midi]

Automatiser les optimisations avec des garde-fous

- La programmation des arrêts et démarrages EC2 avec les filtres offhour et onhour

- La gestion des fuseaux horaires, des calendriers, des tags de planification et des mécanismes d'adhésion ou d'exclusion
- Les actions différées avec mark-for-op et leur sélection ultérieure par marked-for-op
- Les notifications aux propriétaires avec notify, le relais SQS et c7n-mailer
- Les garde-fous avant remédiation : validation humaine, sauvegardes, nouvelle vérification de l'éligibilité et limites du retour arrière
- Atelier pratique : Configurer une politique d'arrêt planifié sur une instance de test et simuler un processus de nettoyage différé avec notification.

[Jour 3 - Matin]

Industrialiser et superviser les politiques

- L'organisation du dépôt Git : conventions de nommage, documentation, paramètres et séparation des environnements
- Les contrôles de CI/CD : validation du schéma, jeux de ressources attendues, revue et déploiement progressif
- Les modes d'exécution sur AWS : lancement local, planification périodique et déploiement dans Lambda
- L'exécution multi-comptes avec c7n-org, les rôles délégués et le ciblage des régions
- La supervision des journaux et métriques, les erreurs de permissions, les limites d'API et les coûts de fonctionnement de l'automatisation
- Atelier pratique : Versionner et valider une politique, déployer son exécution périodique dans le laboratoire et vérifier les traces produites.

[Jour 3 - Après-midi]

Piloter les gains et pérenniser la démarche FinOps

- La définition des indicateurs FinOps : couverture du tagging, ressources optimisées, exceptions et délais de traitement
- La construction d'une situation de référence et la distinction entre économies estimées, coûts évités et gains constatés
- Le rapprochement avec la facturation AWS en tenant compte des variations d'activité, des engagements et des délais de disponibilité des données
- La gouvernance du cycle de vie des politiques : responsabilités, approbations, réévaluation des seuils et expiration des exceptions
- La feuille de route d'amélioration continue et les points de vigilance pour étendre les politiques à d'autres fournisseurs cloud
- Atelier pratique : Assembler un dispositif FinOps complet, de la détection à la remédiation contrôlée, puis présenter les indicateurs de suivi et un plan de déploiement progressif.

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.