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

Mis à jour le 20/03/2026

S'inscrire

Formation certification SailPoint Identity Security Administrator

3 jours (21 heures)

Présentation

La certification SailPoint Certified Identity Security Administrator valide votre capacité à administrer une plateforme IGA et à sécuriser le cycle de vie des identités. Elle s'adresse aux équipes qui doivent industrialiser les provisionings, les revues d'accès et la conformité.

Cette formation vous prépare de façon opérationnelle aux compétences attendues d'un administrateur SailPoint : configuration des connecteurs, modélisation des identités, politiques d'accès et gouvernance. L'objectif est de savoir diagnostiquer et corriger les écarts de droits, tout en garantissant traçabilité et auditabilité.

L'approche est centrée sur la pratique : ateliers guidés, démos de paramétrage, cas d'usage (onboarding/offboarding, recertification, exceptions) et exercices de validation. Vous repartez avec des checklists d'administration, des scénarios de dépannage et un plan de révision aligné sur l'examen.

Objectifs

- Configurer l'environnement SailPoint et les paramètres d'administration essentiels.
- Intégrer des sources d'identités et des applications via connecteurs.
- Mettre en œuvre le provisioning et les workflows de cycle de vie.
- Administrer les politiques d'accès, rôles et contrôles de séparation des tâches.
- Exploiter les campagnes de certification, rapports et journaux d'audit.

Public visé

- Administrateurs IAM/IGA
- Ingénieurs sécurité / Identity Security
- Consultants SailPoint
- Exploitants et équipes support N2/N3

Pré-requis

- Notions solides d’IAM (RBAC, provisioning, SSO)
- Connaissance d’Active Directory et des comptes/attributs
- Bases en LDAP, groupes et droits applicatifs
- Compréhension des enjeux audit et conformité

Pré-requis techniques

- PC avec 8 Go RAM minimum (16 Go recommandé)
- Windows 10/11, macOS ou Linux
- Navigateur récent (Chrome/Firefox/Edge) et accès Internet
- Éditeur de texte et terminal (PowerShell/Bash)

Programme de notre formation Certification SailPoint Certified Identity Security Administrator

[Jour 1 - Matin]

Fondamentaux IAM et prise en main de SailPoint Identity Security Cloud

- Rappels IAM : identités, comptes, droits, rôles, séparation des tâches (SoD)
- Positionnement SailPoint : Identity Security Cloud, IdentityNow, principaux modules
- Navigation console : tenants, menus, objets clés (Identity, Source, Entitlement)
- Pré-requis d’intégration : comptes techniques, API, connectivité, bonnes pratiques de sécurité
- Atelier pratique : Connexion au tenant, exploration guidée et repérage des objets clés.

[Jour 1 - Après-midi]

Sources, connecteurs et agrégation : onboarder une application

- Créer une Source : choix du connecteur, paramètres, authentification et chiffrement
- Schéma et corrélation : accounts, identities, attributs, règles de matching
- Entitlements : collecte, hiérarchies, descriptions, owners et criticité
- Cycles d’agrégation : planification, delta vs full, gestion des erreurs et logs
- Atelier pratique : Onboarder une source de démonstration et lancer une agrégation complète.

[Jour 2 - Matin]

Gouvernance des accès : access profiles, rôles et politiques

- Modéliser les accès : entitlements vs access profiles vs roles
- Construction d’Access Profiles : bundles, attributs, owners, lifecycle et versioning
- Rôles métier et IT : critères d’attribution, règles, exceptions et héritage
- Politiques de conformité : SoD, accès sensibles, alertes et actions de remédiation
- Atelier pratique : Créer un access profile et un rôle, puis tester l’attribution sur des identités.

[Jour 2 - Après-midi]

Workflows de demande d’accès et approbations

- Access Requests : catalogue, items, contraintes, justification et visibilité
- Chaînes d’approbation : managers, owners, approbations multi-niveaux et escalades
- Provisioning : déclenchement, connecteur, suivi d’exécution et reprise sur erreur
- Notifications et traçabilité : événements, audit, preuves et reporting opérationnel
- Atelier pratique : Publier un item au catalogue, soumettre une demande et valider le provisioning.

[Jour 3 - Matin]

Lifecycle et identité : joiner/mover/leaver et gouvernance continue

- Identity Profiles : sources d’autorité, attributs, règles de corrélation et transformations
- Lifecycle States : déclencheurs, transitions, dates, désactivation et réactivation
- Automatisation JML : événements, actions, provisioning/déprovisioning et contrôles
- Gestion des accès orphelins et comptes partagés : détection, ownership et remédiation
- Atelier pratique : Simuler un mover/leaver et vérifier les changements d’accès et de comptes.

[Jour 3 - Après-midi]

Certification des accès, audit et préparation à l’examen

- Access Certifications : campagnes, périmètres, reviewers, décisions et commentaires
- Remédiation : revocation, suivi, exceptions, relances et clôture de campagne
- Audit & reporting : journaux, exports, indicateurs et preuves de conformité
- Révision des thèmes d’examen : pièges fréquents, bonnes pratiques d’administration et troubleshooting
- Atelier pratique : Lancer une campagne de certification, traiter les décisions et générer les preuves.

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.