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

Mis à jour le 19/03/2026

S'inscrire

Formation Certification SailPoint Identity Security Professional

3 jours (21 heures)

Présentation

La certification SailPoint Identity Security Professional valide votre capacité à concevoir, configurer et exploiter une plateforme IGA pour automatiser le cycle de vie des identités, renforcer la conformité et réduire les risques d'accès. Elle s'appuie sur des cas d'usage concrets : onboarding/offboarding, demandes d'accès, recertifications et contrôle des rôles.

Cette formation vise à vous rendre opérationnel sur les fondamentaux SailPoint : modélisation des identités, gouvernance des accès, workflows et intégrations. Vous apprendrez à traduire des exigences métier (séparation des tâches, politiques, audits) en configurations robustes et maintenables.

L'approche est résolument pratique, avec ateliers guidés, démonstrations et exercices de diagnostic. Les livrables incluent une checklist de préparation à l'examen, des scénarios de configuration, et des bonnes pratiques pour sécuriser et industrialiser vos déploiements.

Objectifs

- Identifier les composants clés de l'architecture SailPoint et leurs rôles.
- Configurer les objets cœur : identités, sources, attributs et corrélations.
- Mettre en place des demandes d'accès, approbations et workflows.
- Gérer rôles, politiques et contrôles de conformité (SoD, recertifications).
- Analyser incidents, logs et erreurs pour fiabiliser l'exploitation.

Public visé

- Ingénieurs IAM/IGA et consultants sécurité
- Administrateurs SailPoint et équipes d'exploitation
- Architectes sécurité / responsables gouvernance des accès

Pré-requis

- Notions solides d’IAM : provisioning, authentification, autorisations
- Compréhension des annuaires (AD/LDAP) et des identités
- Connaissances de base en RBAC, SoD et audit
- Lecture de logs et dépannage applicatif

Pré-requis techniques

- PC avec 8 Go RAM minimum (16 Go recommandé)
- Windows 10/11, macOS ou Linux avec navigateur récent
- Accès à un environnement SailPoint de formation et droits d’administration
- Éditeur de texte et terminal (PowerShell, Bash ou équivalent)

Programme de notre formation Certification SailPoint Identity Security Professional Credential

[Jour 1 - Matin]

Fondamentaux IAM et positionnement SailPoint Identity Security

- Rappels IAM/IGA : identité, comptes, rôles, habilitations, séparation des tâches
- Panorama SailPoint : IdentityNow, IdentityIQ, cas d’usage et périmètre de la certification
- Concepts clés : sources, agrégation, corrélation, entitlements, access profiles
- Modèle de gouvernance : policies, approvals, audit, traçabilité
- Atelier pratique : Cartographier un SI cible (sources, populations, applications) et définir les objets IGA attendus.

[Jour 1 - Après-midi]

Modélisation des identités et cycle de vie (Joiner/Mover/Leaver)

- Modèle d’identité : attributs, identifiants, règles de corrélation et qualité des données
- Cycle de vie : événements RH, provisioning/deprovisioning, gestion des exceptions
- Accès par rôles vs accès par profils : critères de choix et impacts opérationnels
- Bonnes pratiques de conception : naming, normalisation, stratégie de tests et rollback
- Atelier pratique : Définir un scénario JML complet et les contrôles associés (création, mobilité, départ).

[Jour 2 - Matin]

Onboarding des sources et gouvernance des accès

- Types de sources : HR, AD, applications, fichiers ; choix des connecteurs et prérequis
- Agrégation : planification, gestion des deltas, traitement des erreurs et réconciliation
- Modélisation des habilitations : entitlements, groupes, permissions, hiérarchies
- Construction des objets de gouvernance : Access Profiles, Roles, règles d'éligibilité
- Atelier pratique : Concevoir un modèle d'accès (entitlements ? access profiles ? rôles) pour une application type.

[Jour 2 - Après-midi]

Demandes d'accès, workflows d'approbation et politiques

- Access Request : catalogue, critères d'éligibilité, justification et traçabilité
- Workflows : approbations (manager, owner, sécurité), escalades, délégations
- Politiques : SoD, accès à risque, contrôles préventifs vs détectifs
- Expérience utilisateur : notifications, SLA, bonnes pratiques de configuration
- Atelier pratique : Définir un workflow d'approbation et une policy SoD sur un cas "finance".

[Jour 3 - Matin]

Certification d'accès (Access Reviews) et conformité

- Types de revues : manager, owner, application, entitlements ; périmètre et fréquence
- Campagnes : ciblage, échantillonnage, priorisation par risque, délégation
- Décisions : approve/revoke, commentaires, preuves et gestion des exceptions
- Remédiation : déclenchement du provisioning, suivi et clôture de campagne
- Atelier pratique : Construire une campagne de revue et définir les règles de remédiation attendues.

[Jour 3 - Après-midi]

Reporting, préparation à l'examen et mise en situation

- Indicateurs clés : couverture des sources, qualité des identités, délais d'approbation, taux de révocation
- Audit & preuves : exigences typiques (SOX/ISO), export et traçabilité des décisions
- Révision des notions de la certification : terminologie, pièges fréquents, scénarios types
- Stratégie d'examen : gestion du temps, lecture des questions, élimination des distracteurs
- Atelier pratique : Mini-examen blanc (questions scénarisées) et correction guidée avec plan d'action de révision.

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.