# C1000-061IBM Security Identity Governance and Intelligence V5.2.5 Deployment

## Objectifs

- Ces professionnels doivent être capables de s'intégrer aux applications métier et aux systèmes cibles, ainsi qu'à d'autres produits et solutions. Ils peuvent accomplir ces tâches avec peu ou pas d'aide de la part de la documentation, de leurs pairs ou de l'assistance.

## Prérequis

- Systèmes d'exploitation LINUX, Unix et Windows
- Différentes technologies de virtualisation (c'est-à-dire KVM, XEN, AWS, AZURE, OPEN Stack)
- Configuration du chiffrement, SSL et HTTPS
- Connaissance générale des réseaux IP, notamment DNS, HTTP
- Navigation dans les arborescences typiques d'informations sur les comptes et les utilisateurs
- Gouvernance de la gestion des identités
- Concepts d'appliance virtuelle
- Structures SQL et bases de données
- Compétences en programmation (c.-à-d. JAVA, REST)
- HTML
- SSO, proxys, OIDC

## Programme

- **Section 1 : Planification de l'architecture et de la conception**
  - Analyser les exigences commerciales, l'environnement et les cas d'utilisation des clients.
  - Déterminez le nombre d'utilisateurs, d'applications (cibles, personnalisées) et le flux des ressources humaines (RH).
  - Déterminez la liste des acteurs qui interagiront avec le système et comment.
  - Planifier et concevoir une architecture et une conception de solutions alignées sur les besoins de l'entreprise.
  - Planifier les besoins d'évolutivité et de disponibilité.
  - Estimer l'effort de mise en œuvre pour le chef de projet.
- **Section 2 : Installation et configuration**
  - Installez et/ou configurez la base de données.
  - Installez le dispositif virtuel IBM Security Identity Governance and Intelligence (IGI).
  - Configurez l'appliance virtuelle IGI (par exemple, NTP, DNS, serveur MAIL, connectivité de base de données, NFS, etc.).
  - Implémentez la haute disponibilité (HA) et la reprise après sinistre (DR).
  - Implémentez des composants réseau supplémentaires tels que des équilibreurs de charge, SSO et des proxys Web.

- Configurez l'appliance virtuelle IGI pour prendre en charge l'application mobile IBM Security Access Request.

- **Section 3 : Intégration des applications et des flux de ressources humaines (RH)**
  - Mettre en œuvre des flux de ressources humaines (RH) (c'est-à-dire configurer des attributs personnalisés, planifier le calendrier d'importation).
  - Planifiez une intégration entre IGI et IBM Security Identity Manager (ISIM), lorsque cela est nécessaire et possible.
  - Installez et intégrez des adaptateurs et des profils pour les applications et systèmes pris en charge.
  - Concevoir et développer des adaptateurs personnalisés pour des applications ou des systèmes, si nécessaire.
  - Configurez les connecteurs d'entreprise.
- **Section 4 : Gouvernance du provisionnement et du cycle de vie**
  - Créez des hiérarchies.
  - Implémentez des règles, des tâches et des tâches personnalisées.
  - Modélisez les attributs de la cible et le mappage des attributs avec les autorisations.
  - Mettre en œuvre des flux de travail.
  - Effectuer le provisionnement et les rapprochements.
- **Section 5 : Modélisation, administration et reporting de la gouvernance**
  - Modélisez les risques (c'est-à-dire les activités commerciales, SoD, violations, atténuations).
  - Effectuez la définition des rôles et l'exploration des rôles.
  - Concevoir, créer et exécuter les campagnes de certification.
  - Concevoir, mettre en œuvre et attribuer des rapports.
  - Gérez les comptes orphelins et sans correspondance.
- **Section 6 : Dépannage, réglage et maintenance**
  - Utilisez les outils de surveillance et les journaux d'historique dans la console d'administration.
  - Identifiez et examinez les fichiers journaux pertinents sur tous les composants, l'appliance virtuelle, l'application IGI et les adaptateurs d'identité.
  - Surveillez et évaluez les performances du système et appliquez les réglages requis.
  - Vérifiez la mise à jour du logiciel et appliquez les packs de correctifs comprenant tous les composants.