

Évaluation Finale : Architecture IAM et Gouvernance des Identités

- **Candidat** : [Nom du binôme]
- **Date** : 17 Mars 2026
- **Durée** : 2h00
- **Documents autorisés** : Support de cours “Architecture et Gouvernance IAM”
- * **Livrable** : un rapport technique par binôme, reprenant point par point le besoin exprimé dans l'énoncé.

Contexte de l'Examen

Environ 80% des violations de données sont causées par des identités compromises ou des accès mal gérés. En tant qu'architecte, vous devez transformer l'Active Directory de **Tailwind Traders** en un véritable système IAM (Identity and Access Management) robuste, respectant le cycle de vie des identités et les principes de gouvernance (IGA).

Mission 1 : Modélisation et Structure (IdM vs AM)

Votre première tâche consiste à différencier la gestion de l'identité (Qui est l'utilisateur ?) de la gestion de l'accès (Que peut-il faire ?).

- **Action 1.1** : Créez une Unité d'Organisation (OU) nommée **Ressources_Critiques**.
- **Action 1.2** : Créez un utilisateur nommé **AuditAdmin**. En vous basant sur le modèle conceptuel de l'IAM, renseignez les **attributs vérifiés** (Ville, Département, Poste) pour cet utilisateur afin de permettre une décision d'accès ultérieure.
- **Question Théorique** : Expliquez brièvement pourquoi la création de cet utilisateur relève de l'IdM et non de l'AM.

Mission 2 : Le Cycle de Vie et Provisioning (IGA)

L'IGA (Identity Governance & Administration) est la couche supérieure qui permet de maîtriser le “chaos des identités”.

- **Action 2.1 (Onboarding)** : Automatisez (via un script PowerShell simple ou une copie de modèle) la création de 3 comptes pour la succursale de **Perth**. Cela correspond à l'étape “Provisioning Automatisé” de la roue de l'IGA.
- **Action 2.2 (RBAC)** : Créez un groupe de sécurité **Perth_Sales**. Appliquez le principe du **RBAC** (Role-Based Access Control) en y ajoutant les utilisateurs en fonction de leur poste.
- **Action 2.3 (Dé-provisioning)** : Un consultant quitte l'entreprise. Désactivez son compte et déplacez-le dans une OU **Archive**. Pourquoi cette étape de révocation est-elle critique pour la conformité ?.

Mission 3 : Authentification et Facteurs de Sécurité

L'identité est devenue le nouveau périmètre de sécurité. Vous devez durcir le “Double SAS” de contrôle.

- **Action 3.1 (Facteurs de type 1)** : Configurez une **FGPP** (Fine-Grained Password Policy) imposant 16 caractères pour le groupe **Perth_Admins**. Quel est le principal risque lié à ce facteur de “connaissance” ?.
- **Action 3.2 (Vers le MFA)** : En vous référant à la taxonomie des 3 facteurs, proposez (par écrit) une solution pour ajouter un facteur de **Type 2** ou **Type 3** à vos administrateurs.
- **Action 3.3 (Hardening)** : Désactivez l'authentification **NTLM** via GPO pour forcer l'usage de protocoles plus modernes. Justifiez cette action par rapport au pilier “Protéger” de l'IAM.

Mission 4 : Audit, Détection et Résilience

Un système IAM sans audit est un passif. Vous devez assurer la visibilité totale.

- **Action 4.1 (Détecter)** : Configurez une stratégie d'audit avancée sur l'OU `Ressources_Critiques` pour détecter toute modification des attributs des comptes. Quel est l'objectif de cette étape dans la stratégie globale ?.
- **Action 4.2 (Résilience)** : Activez la **Corbeille Active Directory**. Supprimez puis restaurez un utilisateur de test.
- **Question de synthèse** : Le support de cours indique que “le MFA n'est pas infailible”. Citez une vulnérabilité spécifique au MFA par SMS que vous devez surveiller.

Barème de Notation

Mission	Points	Compétence évaluée
1. Modélisation	/20	Distinction IdM/AM et gestion des attributs.
2. Cycle de Vie	/30	Provisioning, RBAC et gestion du départ (Offboarding).
3. Authentification	/30	Hardening, facteurs de sécurité et politiques de mots de passe.
4. Audit & IGA	/20	Surveillance des anomalies et résilience du système.
TOTAL	/100	