Étape 1 : Créer une GPO pour l'audit

1. **Ouvrir la console de gestion des stratégies de groupe (GPMC)** :
    - Connectez-vous au **contrôleur de domaine** avec des droits d'administrateur.
    - Cliquez sur **Démarrer**, tapez **gpmc.msc**, puis appuyez sur **Entrée** pour ouvrir la console de gestion des stratégies de groupe (**GPMC**).
2. **Créer une nouvelle GPO** :
    - Dans la console **GPMC**, développez l'arborescence de votre domaine :
        - **Forêt** → **Domaines** → **[Nom de votre domaine]**.
    - Faites un clic droit sur **[Nom de votre domaine]**, puis sélectionnez **Créer un objet GPO dans ce domaine et le lier ici**.
    - Nommez cette nouvelle GPO **Audit Groupes et Sessions**, puis cliquez sur **OK**.

Étape 2 : Configurer la GPO pour l'audit

1. **Modifier la GPO** :
    - Dans **GPMC**, faites un clic droit sur la GPO **Audit Groupes et Sessions**, puis cliquez sur **Modifier**.
2. **Configurer l'audit des groupes de sécurité** :
    - Dans l'éditeur de la stratégie de groupe, accédez à :
      Configuration ordinateur → **Stratégies** → **Paramètres Windows** → **Paramètres de sécurité** → **Stratégie d'audit avancée** → **Gestion des comptes** → **Audit des modifications des groupes de sécurité**.
    - Double-cliquez sur **Audit des modifications des groupes de sécurité**, sélectionnez **Succès** et **Échecs**, puis cliquez sur **Appliquer** et **OK**.
3. **Configurer l'audit des ouvertures et fermetures de session** :
    - Toujours dans l'éditeur de stratégie de groupe, allez à :
      Configuration ordinateur → **Stratégies** → **Paramètres Windows** → **Paramètres de sécurité** → **Stratégie d'audit avancée** → **Connexion/fermeture de session**.
    - Double-cliquez sur **Audit des ouvertures de session** et cochez **Succès** et **Échecs**. Cliquez sur **Appliquer** et **OK**.

- Ensuite, double-cliquez sur **Audit des fermetures de session** et cochez également **Succès** et **Échecs**. Cliquez sur **Appliquer** et **OK**.

4. **Fermer l'éditeur** une fois toutes les configurations appliquées.

Étape 3 : Appliquer la GPO

1. **Forcer la mise à jour des stratégies de groupe** :
   - Ouvrez une **Invite de commandes** ou **PowerShell** avec des privilèges administratifs sur le contrôleur de domaine ou sur les machines cibles.
   - Exécutez la commande suivante pour appliquer immédiatement la GPO :

bash

Copier le code

gpupdate /force

Étape 4 : Vérifier l'audit via l'observateur des événements

1. **Ouvrir l'Observateur des événements** :
   - Sur le serveur, cliquez sur **Démarrer**, tapez **eventvwr.msc**, puis appuyez sur **Entrée** pour ouvrir l'**Observateur des événements**.
2. **Accéder aux journaux de sécurité** :
   - Dans l'Observateur des événements, développez l'arborescence suivante :
     - **Journaux Windows** → **Sécurité**.
3. **Rechercher les événements liés à la gestion des groupes et aux sessions** :
   - Dans le journal de sécurité, vous verrez des événements relatifs à l'ouverture et fermeture de session, ainsi qu'aux modifications des groupes de sécurité.
   - **ID d'événements** spécifiques à rechercher :
     - **ID 4728** : Un membre a été ajouté à un groupe de sécurité global.
     - **ID 4729** : Un membre a été supprimé d'un groupe de sécurité global.
     - **ID 4624** : Connexion réussie (ouverture de session).
     - **ID 4634** : Fermeture de session.

Étape 5 : Créer une vue personnalisée pour surveiller les événements

1. **Créer une vue personnalisée** :
    - Dans **l'Observateur des événements**, faites un clic droit sur **Journaux Windows → Sécurité** et sélectionnez **Créer une vue personnalisée**.
    - Dans la fenêtre **Créer une vue personnalisée**, configurez les paramètres suivants :
        - **Période** : Sélectionnez la période qui vous intéresse (par exemple, **Dernières 24 heures**).
        - **Journal** : Cochez **Journaux de sécurité**.
        - **Source d'événements** :
            - Pour Windows Server 2019 : Sélectionnez **Microsoft Windows Security-audit**.
            - Pour les versions antérieures à Windows Server 2019 : Sélectionnez **Security-audit**.
        - **ID des événements** : Entrez les ID suivants : **4728, 4729, 4624, 4634**.
2. **Enregistrer la vue** :
    - Cliquez sur **OK**, puis donnez un nom à la vue, par exemple **Audit Groupes et Sessions**.
    - Cliquez sur **OK** pour enregistrer la vue personnalisée.
3. **Vérifier les résultats** :
    - Sélectionnez la vue personnalisée que vous venez de créer et observez les événements pour voir si les opérations d'audit sont correctement enregistrées (par exemple, tentatives d'ouverture de session, modification des groupes de sécurité, etc.).

Résumé des paramètres configurés :

- **Gestion des groupes de sécurité** : Audit des succès et des échecs sur les modifications des groupes de sécurité.
- **Ouverture/Fermeture de session** : Audit des succès et des échecs pour les ouvertures et fermetures de session.

Étapes de validation :

- **Accéder à l'Observateur des événements**.
- **Rechercher les événements** avec les **ID 4728, 4729, 4624, 4634**.

- **Créer une vue personnalisée** pour surveiller les événements d’audit des groupes et des sessions.