Audit d'un système de fichiers

Objectif : Récolter des évènements sur des tentatives infructueuses

Sur **AD1**, créer un dossier **C:\Informatique** puis accédez aux **Propriétés** du dossier

Cliquer sur l'onglet **Partage** puis sur le bouton **Partage avancé**

Cocher la case **Partager ce dossier** puis cliquer sur le bouton **Autorisations**

Supprimer le groupe **Tout le monde**

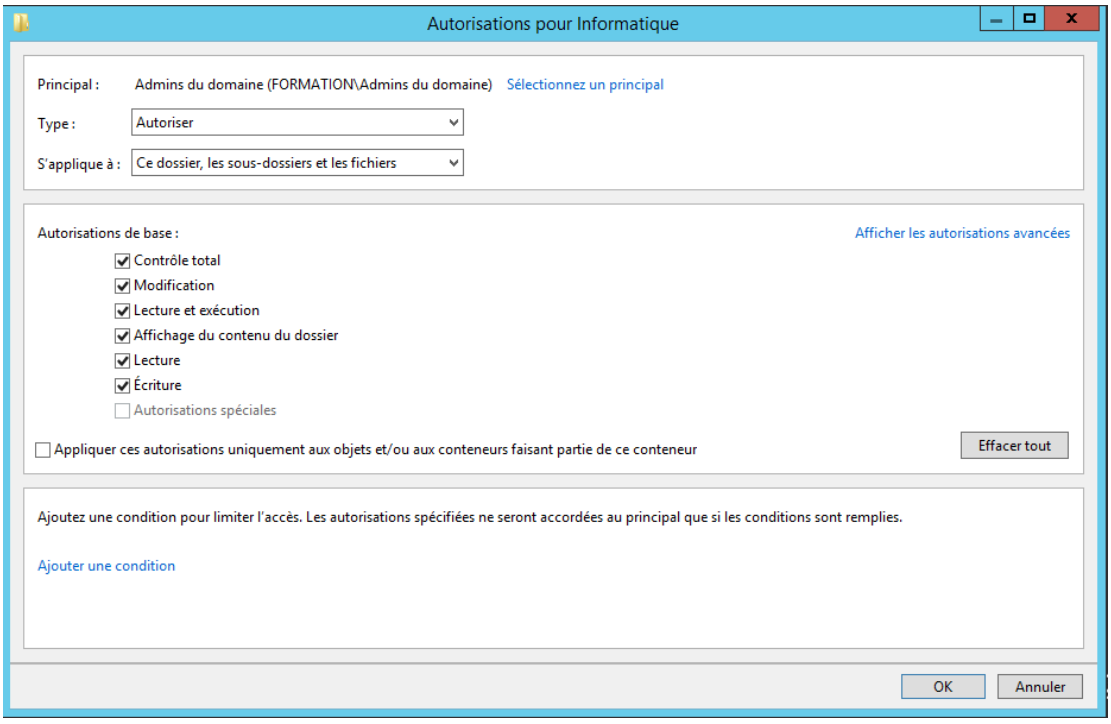
Ajouter le groupe **admins du domaine** avec un Accès en **Contrôle Total**

Cliquer sur l'onglet **Sécurité** puis sur le bouton **Avancé**

Dans l'onglet **Autorisations**, cliquer sur **Désactiver l'héritage** puis sur **Supprimer toutes les autorisations héritées de cet objet**

Cliquer sur le bouton **Ajouter** puis sur le lien **Sélectionner un principal**

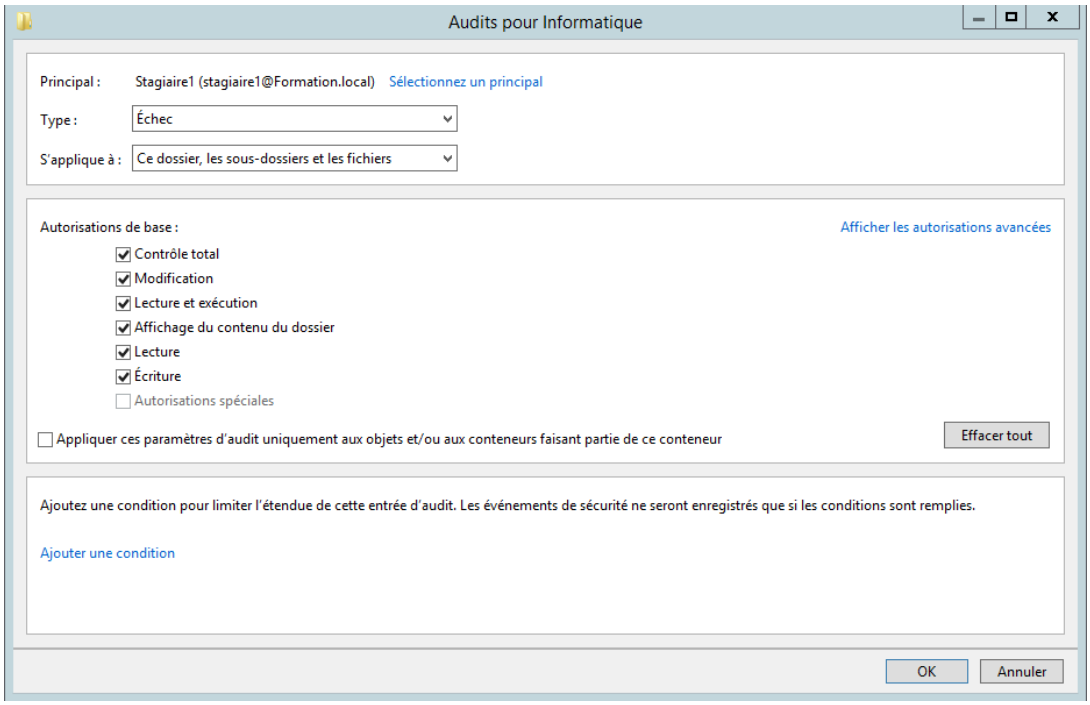
Dans la fenêtre de sélection, choisir **admins du domaine** puis lui donner les droits de **Contrôle totale**



Dans l'onglet **Audit**, cliquer sur **Ajouter**

Cliquer sur le lien **Sélectionner un principal** puis sélectionner **Stagiaire1**

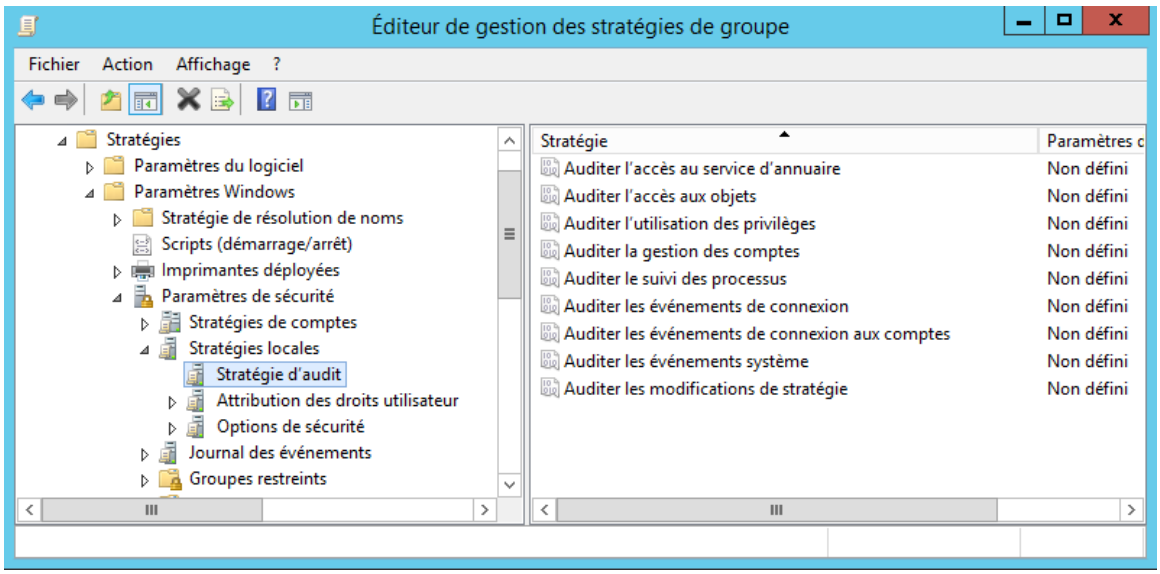
Dans la liste déroulante **Type**, choisir **Echec** puis activer le droit **Contrôle Total**



Lancer la console **Gestion de stratégie de groupe** puis créer une **nouvelle stratégie** nommée **Audit dossier Info**

Clic-droit sur la stratégie crée puis cliquer sur **Modifier**

Développer **Configuration ordinateur > Stratégies > Paramètres Windows > Paramètres de sécurité > Stratégies locales > Stratégies d'audit**



Double-clic sur **Auditer l'accès aux objets**

Cocher **Définir ces paramètres de stratégie** puis cocher **Echec**

Fermer la console Editeur de stratégie en validant par **OK**

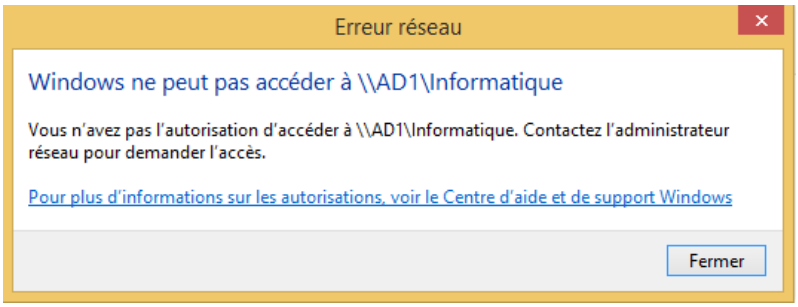
Lier la stratégie **Audit dossier Informatique** à l'OU **Domain Controllers**

Lancer une **invite de commande** sur **AD1** puis exécuter la commande : `gpupdate /force`

Ouvrir une session sur **CL8-02** en tant que **Stagiaire1**

Essayer d'accéder au dossier partagé **Informatique** sur **AD1**

Un message d'avertissement signale un accès refusé



Sur **AD1**, lancer la console **Gestion de l'ordinateur** puis développer **Observateur d'évènements > Journaux Windows**

Visualiser le journal d'évènements **Sécurité**

Ouvrez l'évènement qui référence la tentative d'accès de **Stagiaire1** (ID 4634)

A chaque tentative de **Stagiaire1**, un évènement est créé dans le journal