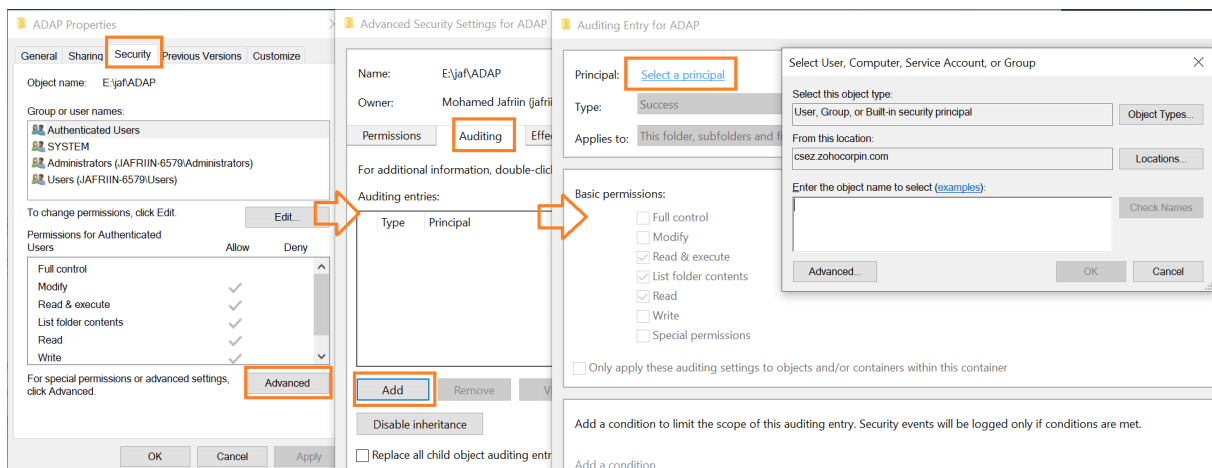


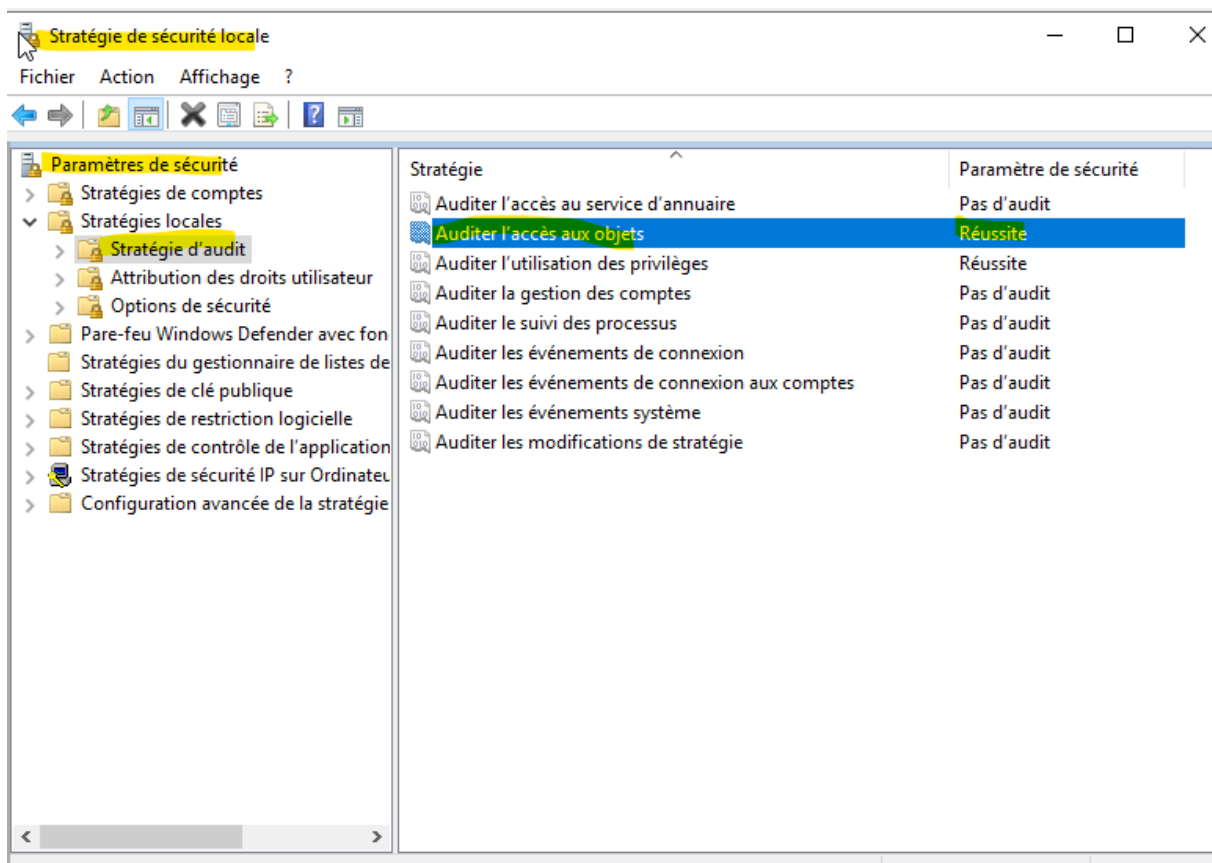
Tout d'abord, il faut créer l'audit sur le fichier.



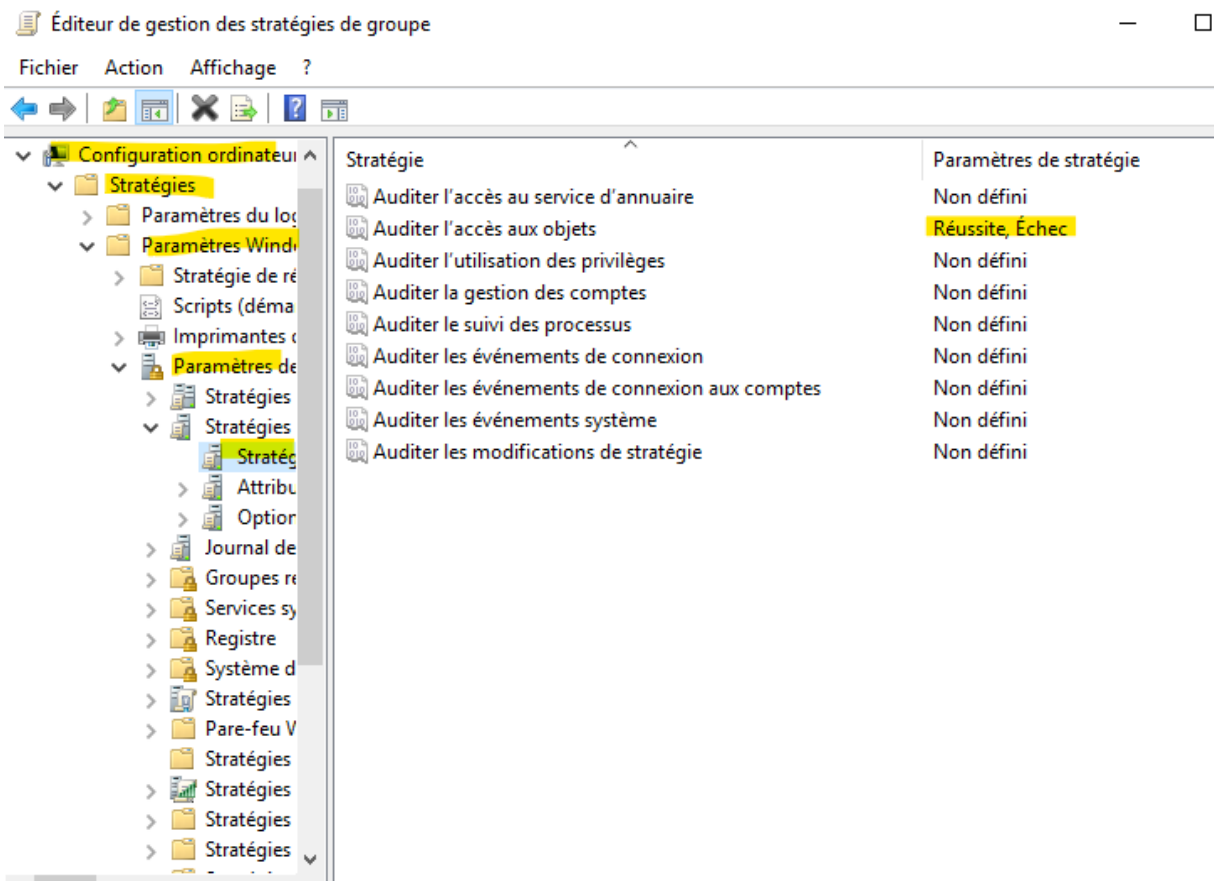
Mettre « tout le monde »

Puis mettre les permissions qu'il faut

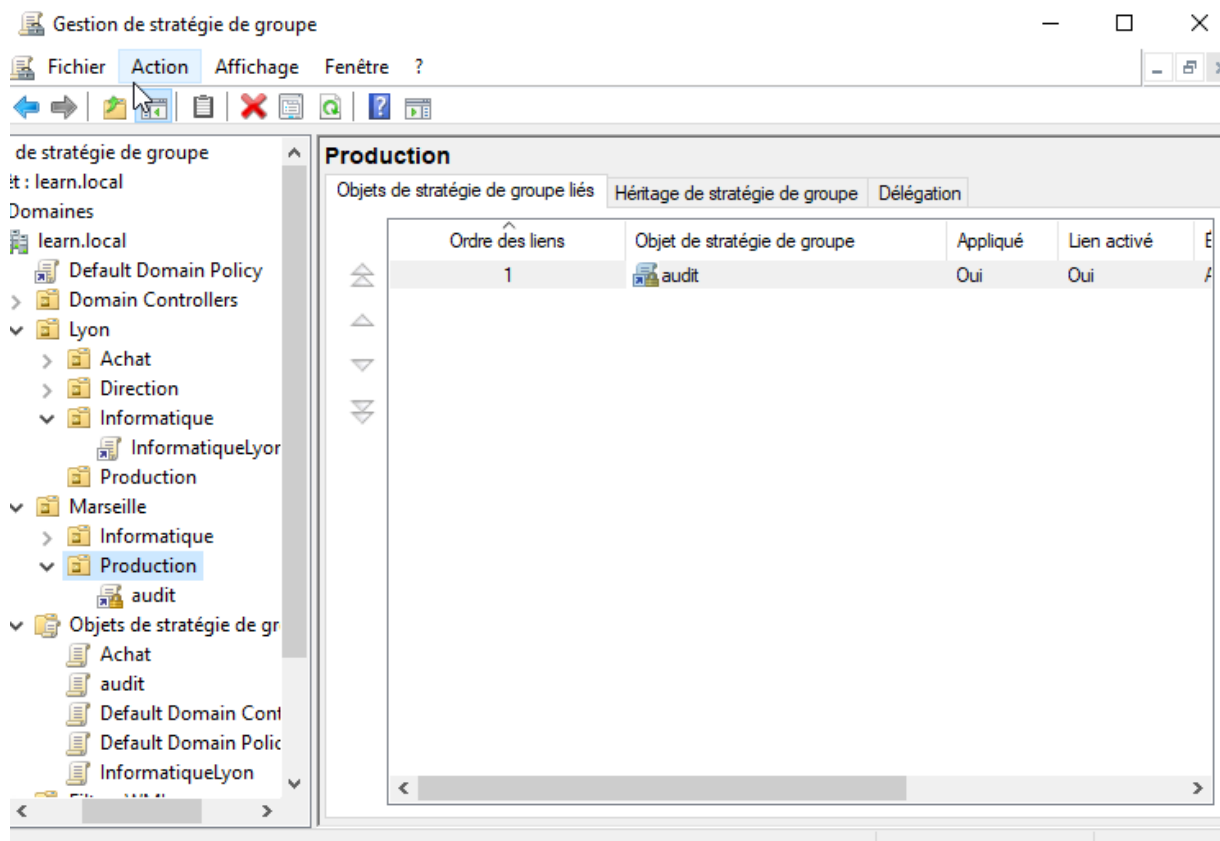
Une fois que c'est fait, il faut mettre l'audit sur l'accès aux objets en réussite



Puis créer une GPO « audit », l'appliquer et la modifier pour appliquer le même paramètre que ci-dessus



Et mettre la GPO dans le dossier production ou il y a l'utilisateur qui va tester



Ensuite Gpupdate /force le server et le client

Et dans l'observateur d'événements, il y a l'alerte :

The screenshot shows the Windows Event Viewer application. The left pane displays the 'Security' log. The main pane shows a list of events, with event 4659 selected. The details pane for event 4659 is open, showing the following information:

Niveau	Date et heure	Source	ID de l'événement	Catégorie de l'événement
Information	5/16/2024 1:40:20 PM	Microsoft Wi...	4658	File System
Information	5/16/2024 1:40:20 PM	Microsoft Wi...	4690	Handle Manip...
Information	5/16/2024 1:40:20 PM	Microsoft Wi...	4659	File System
Information	5/16/2024 1:40:20 PM	Microsoft Wi...	5145	Detailed File S...
Information	5/16/2024 1:40:20 PM	Microsoft Wi...	5145	Detailed File S...

Événement 4659, Microsoft Windows security auditing.

Général Détails

Informations sur le processus :
ID du processus : 0x4

Informations sur la demande d'accès :
ID de la transaction : {00000000-0000-0000-0000-000000000000}
Accès : DELETE
ReadAttributes

Masque d'accès : 0x10080
Privilèges utilisés pour les vérifications d'accès : -

Journal : Sécurité
Source : Microsoft Windows security Connecté : 5/16/2024 1:40:20 PM
Événement : 4659 Catégorie : File System
Niveau : Information Mots-clés : Succès de l'audit
Utilisateur : N/A Ordinateur : DC1.learn.local
Opcode : Informations
Informations : [Aide sur le Journal](#)

(ci-dessus une alerte de suppression de fichier)

Autre xemple avec un contrôle de lecture

The screenshot shows the Windows Event Viewer application. The left pane displays the 'Security' log. The main pane shows a list of events, with event 4656 selected. The details pane for event 4656 is open, showing the following information:

Niveau	Date et heure	Source	ID de l'événement	Catégorie de l'événement
Information	5/16/2024 2:23:54 PM	Microsoft Wi...	5156	Filtering Platf...
Information	5/16/2024 2:23:54 PM	Microsoft Wi...	5156	Filtering Platf...
Information	5/16/2024 2:23:53 PM	Microsoft Wi...	4656	File System
Information	5/16/2024 2:23:53 PM	Microsoft Wi...	4658	File System
Information	5/16/2024 2:23:53 PM	Microsoft Wi...	4663	File System
Information	5/16/2024 2:23:53 PM	Microsoft Wi...	4663	File System
Information	5/16/2024 2:23:53 PM	Microsoft Wi...	4656	File System
Information	5/16/2024 2:23:53 PM	Microsoft Wi...	4658	File System
Information	5/16/2024 2:23:53 PM	Microsoft Wi...	4690	Handle Manip...
Information	5/16/2024 2:23:53 PM	Microsoft Wi...	4658	Registry

Événement 4656, Microsoft Windows security auditing.

Général Détails

ID de la transaction : {00000000-0000-0000-0000-000000000000}
Accès : READ_CONTROL
SYNCHRONIZE
Écriture données (ou ajout fichier)
Ajout données (ou ajout sous-répertoire ou créer instance de canal)

Journal : Sécurité
Source : Microsoft Windows security Connecté : 5/16/2024 2:23:53 PM
Événement : 4656 Catégorie : File System
Niveau : Information Mots-clés : Échec de l'audit
Utilisateur : N/A Ordinateur : DC1.learn.local
Opcode : Informations
Informations : [Aide sur le Journal](#)