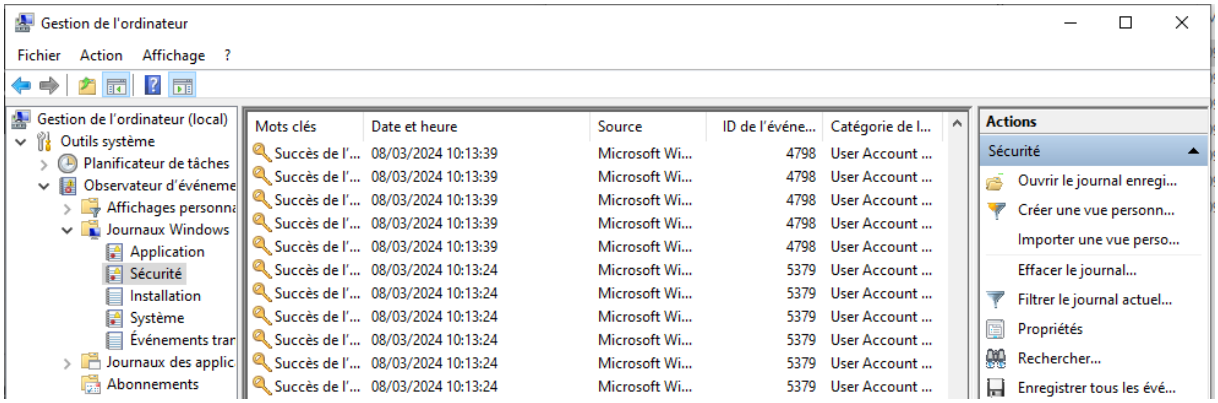
Les Audits

I. Introduction

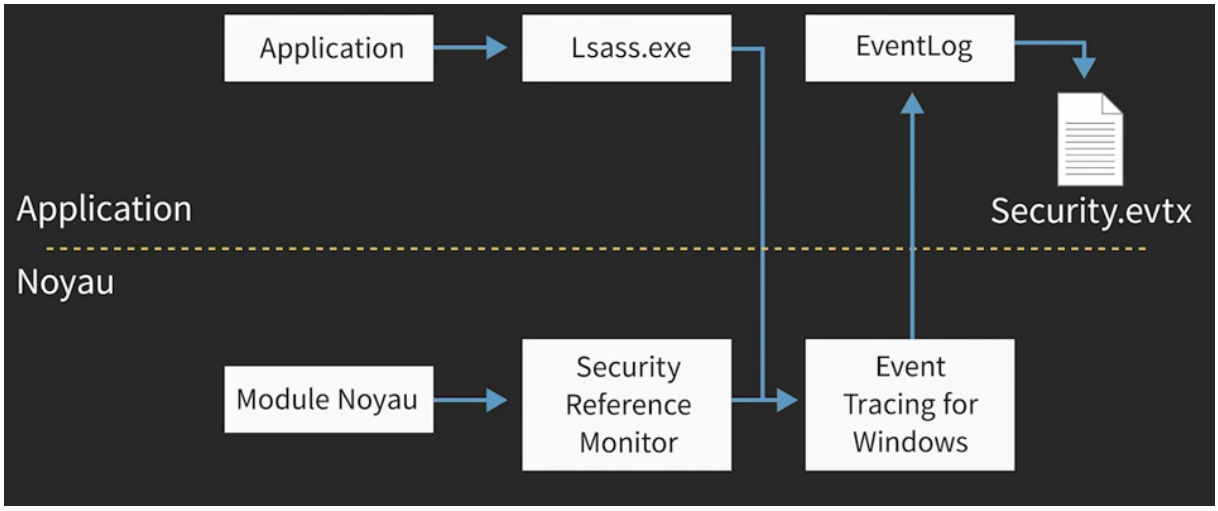
Il est primordial de mettre en place des audits d'évènement, afin de surveiller votre Windows. Ceux-ci permettent de détecter toutes les activités de votre système (connexion, accès, lancement d'application, tentative de modification des droits, …)

L'élément le plus visible va être le journal de sécurité :



Il regroupe des événements écrits dans le fichier security.evtx, dont seuls quelques utilisateurs ont le droit de le lire (SYSTEM, les administrateurs et les Opérateurs de journaux d'événements)

Fonctionnement :



Il existe 2 configurations d'audit :

- Configuration héritée qui existe depuis la première version de Windows NT et qui est toujours présente. Il est aujourd'hui déconseillé de l'utiliser

- Configuration avancée qui est apparu depuis Windows Vista qui permet une configuration beaucoup plus fine des audits. C'est celle-ci qu'il est à privilégier aujourd'hui

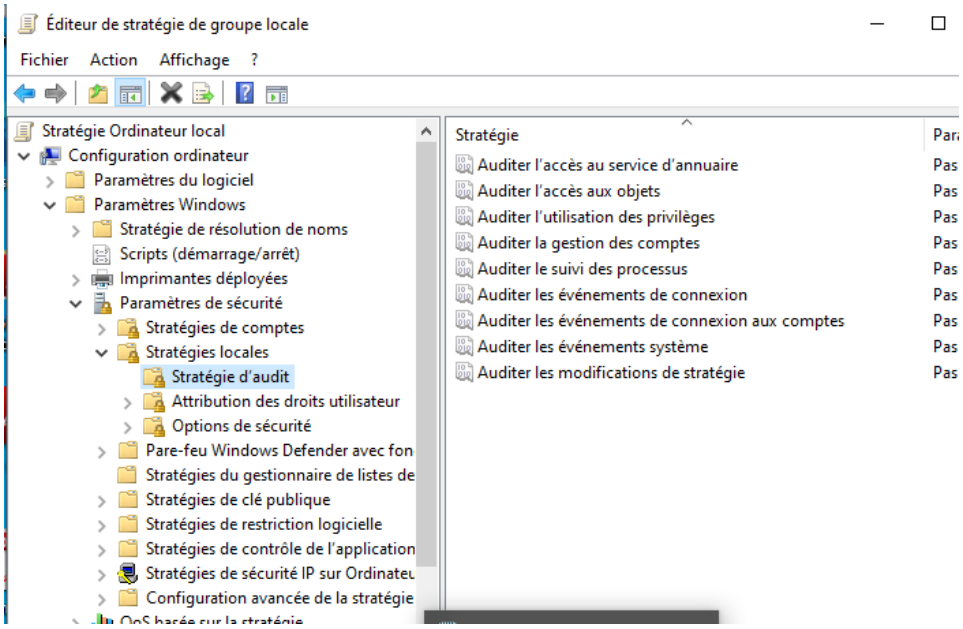
Dans tous les cas, il ne faut pas utiliser les 2 systèmes de configuration en même temps

II. Mise en place

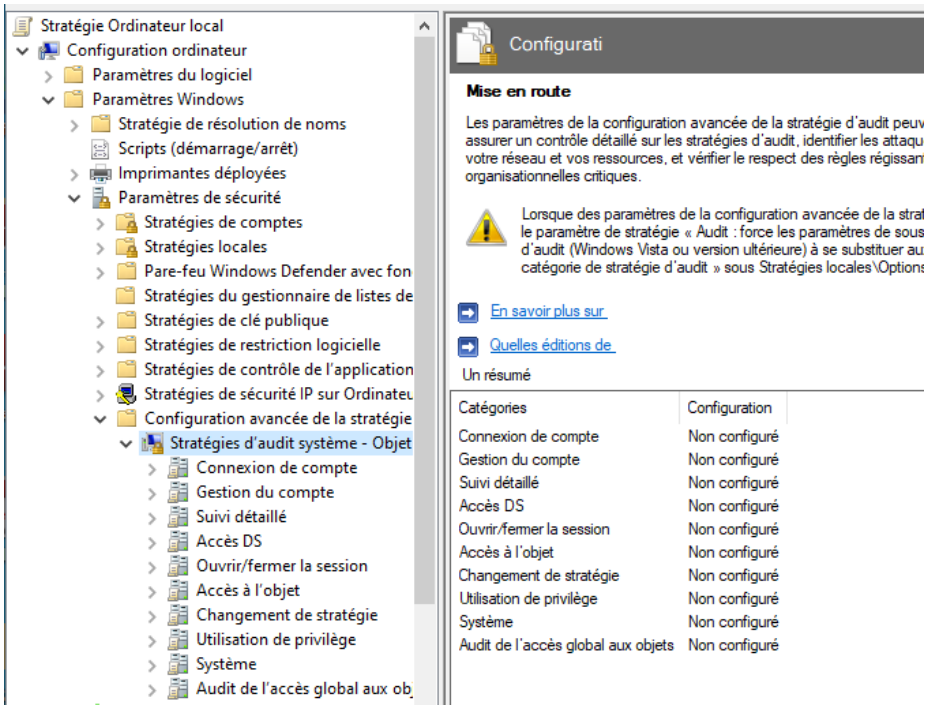
Il existe 2 moyens de définir nos audits :

- Par l'intermédiaire d'une stratégie, la plupart du temps dans un domaine, mais utilisable aussi sur une machine cliente. Il est possible d'importer et d'exporter des politiques d'audit.
- Par l'intermédiaire d'une commande grâce à l'outil auditpol.exe

Ici la stratégie de configuration héritée (à proscrire) :



Ici la stratégie de configuration avancée :



Cette dernière stratégie permet de consigner dans le journal selon si l'action fut un succès, un échec, ou les 2.

1. Gestion des audits par la commande

- ✓ Ouvrez un CMD en tant qu'administrateur

La commande permettant de visualiser la liste des catégories auditées est la suivante :

```
auditpol.exe /get /category :*
```

- ✓ Activez par le succès et l'échec, la stratégie de validation des informations d'identification, et vérifiez à l'aide de la commande, la prise en compte de cette validation

La commande permettant d'activer un audit est la suivante :

```
auditpol.exe /set /subcategory:'Nom_de_la_catégorie'
/success:enable_ou_disable  /failure:enable_ou_disable
```

- ✓ Activez en commande, la surveillance des évènements Plug and Play en succès et en échec, puis vérifiez la prise en compte de celle-ci dans vos stratégies

- ✓ Exportez vos paramètres d'audit (option /backup) dans un fichier .csv, et réimportez le dans une nouvelle machine

2. Auditer l'accès aux ressources

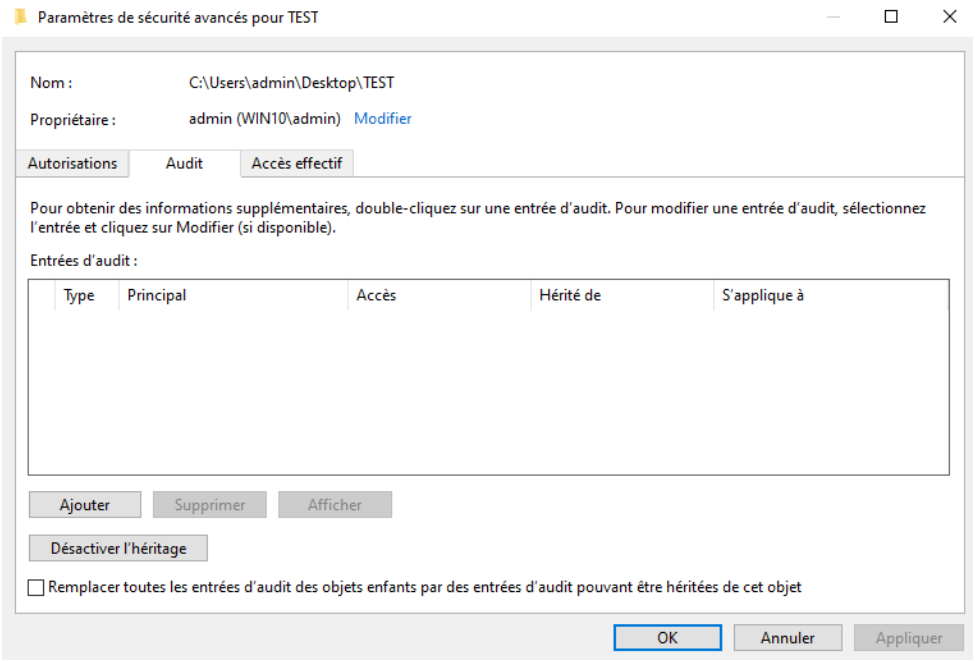
Cette catégorie permet d'auditer les accès aux fichiers, aux dossiers, et à la base de registre. Voici les principaux évènements et leur code (la liste est non exhaustive et vous pouvez trouver la liste complète sur le site de Microsoft) :

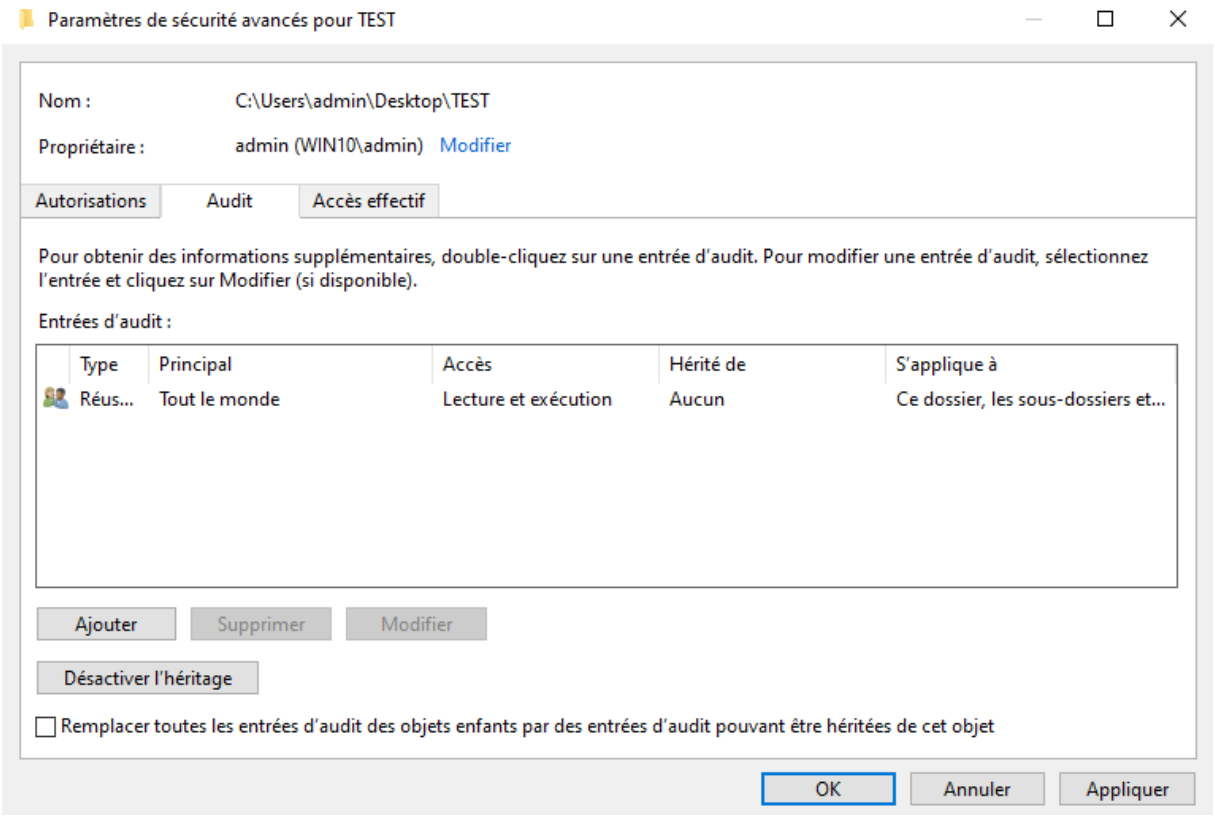
- 4656 (S/E) : Ouverture ou tentative d'ouverture d'un objet
- 4658 (S) : Fermeture d'un objet
- 4670 (S) : Changement de permissions
- 4663 (S) : Utilisation du handle (lire ou écrire dans un fichier)
- 4659,4660 (S) : Suppression
- 4667 (S) : Modification d'une valeur du registre

Pour les vérifications suivantes, nous allons activer les audits des accès à l'objet en succès et échec pour « Auditer le système de fichiers », « Auditer la manipulation de handle », et « Auditer le registre »

- ✓ Mettez en place cette configuration
- ✓ Créez un dossier nommé « Test » à la racine de votre système

Par défaut, l'audit de tous vos dossiers n'est pas activé, nous allons devoir le faire manuellement. Ceci se déroule dans l'onglet sécurité de l'objet puis « Avancé ». L'audit fonctionne de la même manière que les contrôles d'accès mais ne fonctionne plutôt que comme un filtre. L'héritage reste valable dans les audits





- ✓ Créez un nouveau fichier dans votre dossier Test
- ✓ Editez le et ajoutez quelques lignes de texte
- ✓ Enregistrez et fermez votre fichier
- ✓ Supprimez-le
- ✓ Rendez-vous dans l'observateur d'évènements et vérifiez la remontée de vos actions ainsi que le code concerné
- ✓ Etudiez les messages affichés et retrouvez vos informations

- ✓ Créez une nouvelle clé registre Test ainsi qu'une clé avec une valeur quelconque et de la même manière activez l'audit
- ✓ Modifiez votre clé
- ✓ Observez les audits qui ont été relevés par vos actions

3. Auditer les ouvertures de session

Voici les évènements consignés et leur code :

- 4776 (S/E) : Validation des informations d'authentification, qui valide typiquement les mots de passe (ne concerne que les comptes locaux)
- 4624 (S) : Ouverture de session réussie
- 4625 (E) : Echec d'ouverture de session
- 4648 (S) : Utilisation d'informations d'authentification explicites (mot de passe par exemple)
- 4647 (S) : Début de fermeture de session
- 4634 (S) : Fermeture de session

Afin de vérifier ceci, activez en succès et en échec, la stratégie « Auditer la validation des informations d'identification » dans Connexion de compte ainsi que « Auditer l'ouverture de session » dans la catégorie Ouvrir/fermer la session

- ✓ Créez un compte utilisateur « testuser » avec le mot de passe de votre choix

- ✓ Depuis la commande, lancez une session CMD.EXE en tant que testuser (commande runas)

- ✓ Fermez ce CMD.EXE

- ✓ Relancer ce même lancement de CMD.EXE mais en vous trompant intentionnellement de mot de passe

- ✓ Lancez votre observateur des évènements et identifiez les messages et les codes du journal en correspondance à vos actions précédentes (observez les détails)

4. Auditer l'utilisation des privilèges

Voici les évènements consignés et leur code :

- 4672 (S) : Assignation des privilèges lorsque l'utilisateur ouvre sa session
- 4673 (S/E) : Appel aux services sensibles (de sécurité par exemple)
- 4674 (E) : Opération sur objet sensible

Afin d'effectuer les vérifications, activez en succès et en échec, la stratégie « Auditer l'utilisation de privilèges sensibles » dans la catégorie Utilisation de privilège

- ✓ Tentez, en commande, de prendre possession du fichier C:\Windows\notepad.exe (commande takeown)
- ✓ Vérifiez le journal de sécurité et identifiez les évènements correspondants

5. Auditer l'activité du système

Voici les évènements consignés et leur code :

- 4688 (S) : Nouveau processus démarré
- 4689 (S) : Processus terminé
- 4608 (S) : Démarrage de Windows (Lsass.exe)
- 4616 (S) : Changement d'heure

Afin de vérifier ceci, activez en succès les stratégies « Auditer la création du processus » et « Auditer la fin du processus » dans la catégorie Suivi détaillé

- ✓ Lancez notepad.exe en invite de commande administrateur

- ✓ Analysez le journal de sécurité et relevé les messages correspondant à vos actions

- ✓ Quelle est la classification de sécurité de cet évènement ? Expliquez pourquoi

- ✓ Relancez dans CMD, cette fois ci en mode utilisateur, le processus notepad.exe

- ✓ Analysez la classification de sécurité de l'évènement et vérifiez votre hypothèse précédente

- ✓ Visualisez le processus parent

6. Auditer le changement des stratégies de sécurité

Voici la liste des évènements générés et leur code :

- 4719 (S) : Changement de la politique d'audit
- 4739 (S) : Changement de la politique d'authentification (longueur des mots de passe, complexité, …)
- 4717 (S) : Ajout d'un privilège d'accès à un utilisateur
- 4718 (S) : Retrait de l'accès à la machine

Activez en succès les stratégies « Auditer les modifications de la stratégie d'audit » et « Auditer la modification de stratégie d'authentification » dans la catégorie Changement de stratégie

Activez une stratégie d'audit quelconque

Désactivez là immédiatement derrière

Retirez à « tout le monde » l'accès à cet ordinateur à partir du réseau

Activez une longueur minimale de mot de passe de 8 caractères

Vérifiez dans le journal de sécurité vos actions précédemment réalisées