http://WWW.CABARE.NET ©

Stratégies et GPO Audit sous Windows 10 - 2026 - 2012R2 – sys 26 – cours -

Stratégies Audit Windows 10 et Domaine 2016

Michel Cabaré – Ver 2.6 – Juin 2017-

Stratégies et GPO Audit sous Windows 10- 2012R2 - 2016

Cours

Michel Cabaré – Ver 2.6 – Juin 2017

www.cabare.net ©

La formation que vous suivez, à pour but de vous initier avec les logiciels Microsoft Windows 2016-2012R2 Serveur et clients Windows 10- 7.

Ce Support à pour but de vous fournir un certain nombre d'éléments concernant soit des manipulations, soit des notions théoriques concernant la gestion de réseaux locaux

Il ne peut en aucun cas se substituer à la participation à la formation, ni à tout ou partie de la documentation fournie avec le logiciel.

En effet, **et c'est là sa vocation première**, ce document doit **"servir de support à la prise de notes en formation, et sera donc avantageusement complété par vos soins"**. Son but est de permettre une présentation de vos notes plus structurée et donc plus facilement utilisable ensuite.

Bon Travail

Michel Cabaré

TABLE DES MATIÈRES

STRATEGIES LOCALES - AUDIT

Audit évènement – audit Ressource:

Il est possible par un audit de suivre les évènements qui surviennent de la part d'un utilisateur, ou du système d'exploitation, sur **une machine donnée**. Chaque événement est consigné dans un des journaux, appelé **journal de sécurité, qui ne contient pas uniquement les évènements d'AUDIT…** Une **stratégie d'audit**, peut définir soit

- les **types d'événement** à surveiller
- soit les **types de ressources**

Stratégie d'audit, et **types d'événement** à surveiller.

Dans la liste suivante les moins importants sont entre parenthèses ():

- **Gestion des comptes** : un compte est crée, modifié (mot de passe…)
- **(Suivi des processus)** : uniquement pour les développeurs…
- **(Connexion)** : enregistre les sessions sur le poste, que celle-ci soient locales ou via le réseau, qu'elles utilisent un compte local ou de domaine, (l'audit est posé sur la station)
- **Connexion compte** : enregistre les demandes d'identification. Si la demande d'ouverture de session se fait sur le domaine, elle est reçue par un contrôleur de domaine, et l'audit doit être posé sur le contrôleur. Si elle est locale, l'audit doit être posé localement
- **(Evènements système)** : démarrage ou arrêt du poste…
- **(Modification de stratégie)** : modification aux options de sécurité ou aux stratégies …. D'audit
- **Utilisation de privilèges** : comme la possibilité de modifier l'heure système, ou lorsque un administrateur s'approprie un fichier

Stratégie d'audit, et **types de ressources** à surveiller

- **Accès à AD** : un utilisateur accède à AD, l'audit doit être posé sur l'objets AD
- **Accès aux objets** : un utilisateur accède à une ressource fichier, dossier, imprimante. (**N.B**: ensuite l'audit doit être posé sur chaque objet à auditer via les permissions NTFS…)

De manière générale donc, pour installer un audit, il va falloir :

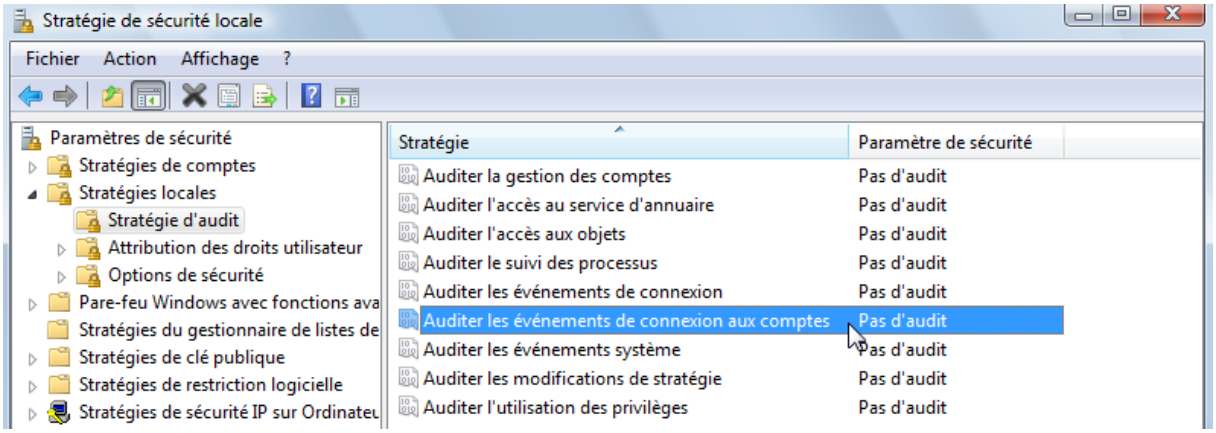
1. Choisir les postes où installer l'audit
2. Déterminer les évènements à auditer
3. Indiquer si on veut auditer les succès ou les échecs

Installer un Audit sur évènement – 10 - Seven

Lorsque l'on veut auditer un évènement, on peut en général auditer aussi bien les **accès réussit**, que les **accès en échec**, les deux n'ont pas la même finalité, et on effectuera toujours un audit minimal afin de faciliter ensuite la lecture du journal d'évènement…

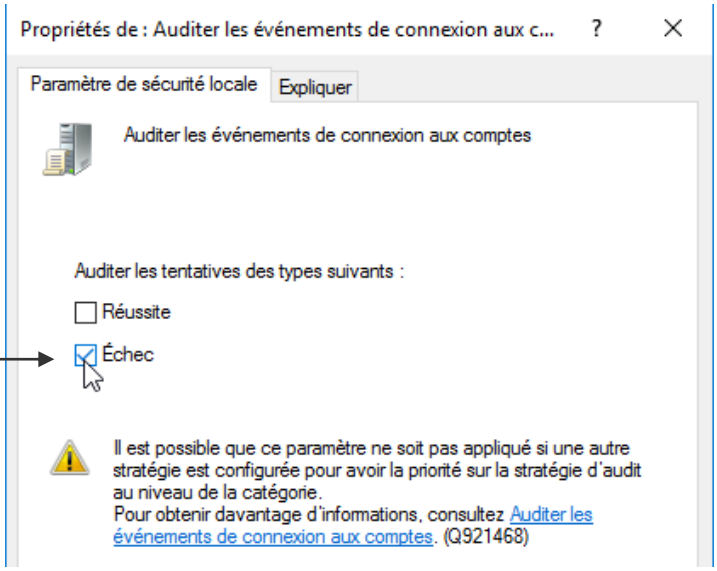
Il faut passer par les **Stratégies de sécurités locales**,

sous Windows 10 **Stratégies locales / Stratégies d'audit**

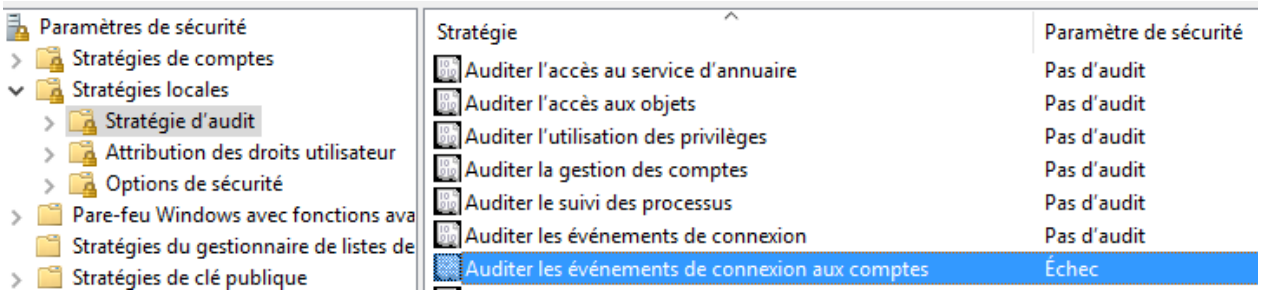


par exemple sur **évènements de connexion aux comptes**

et en demandant d'auditer les **Réussites** et/ou les **Echec**…



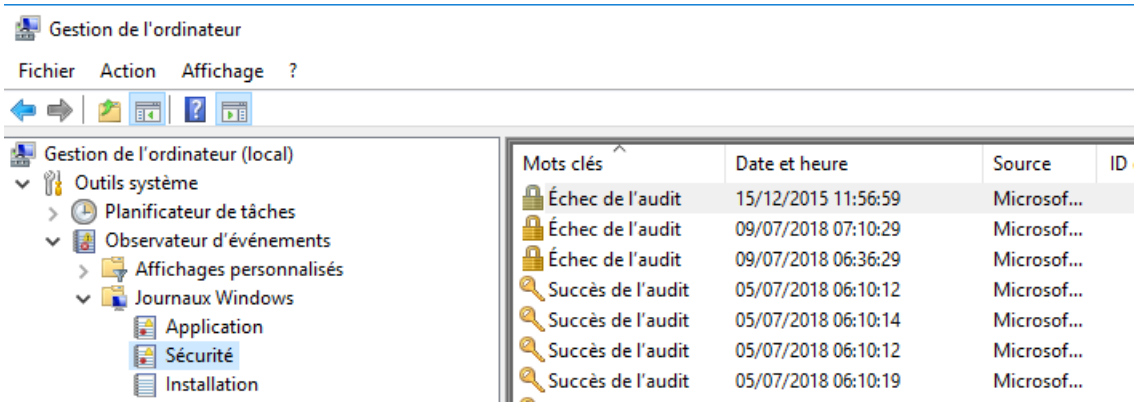
par exemple on souhaite ici pister les tentatives d'accès avec un mot de passe erroné… pour obtenir donc après une tentative d'ouverture erronée



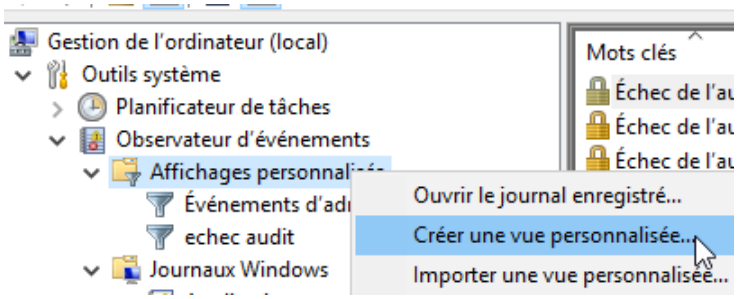
Se préparer dans l'observateur d'évènement

Accessible via Gérer l'ordinateur,

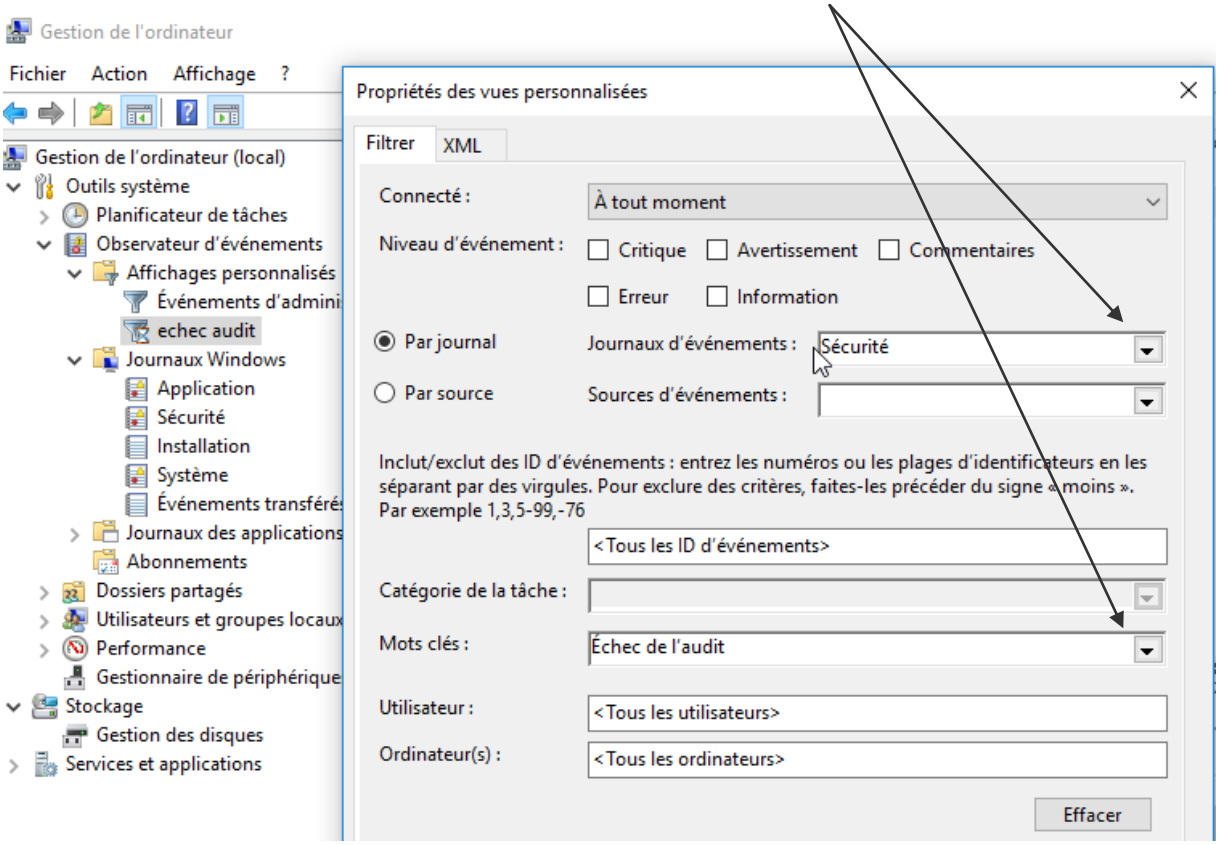
Dans l'observateur d'évènement, les audits sont par défaut enregistrées dans les **Journaux Windows, Sécurité**



On peut si on le souhaite se créer un **journal personnalisé** pour que la lecture soit moins verbeuse

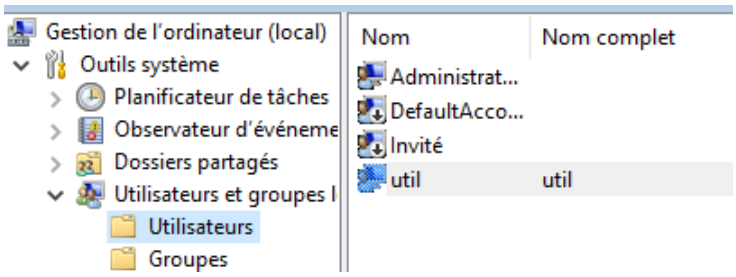


Qui consignerais uniquement les echecs de l'audit

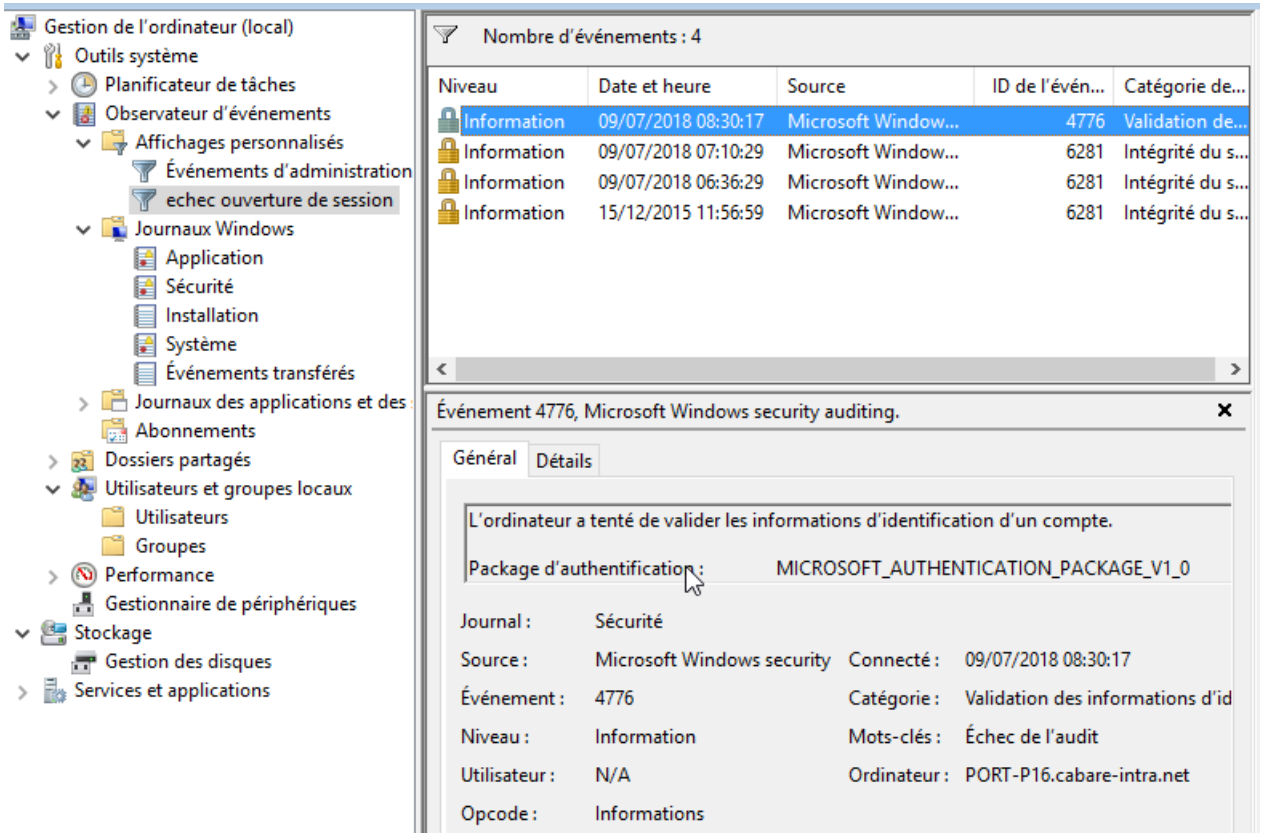


Voir un évènement audité

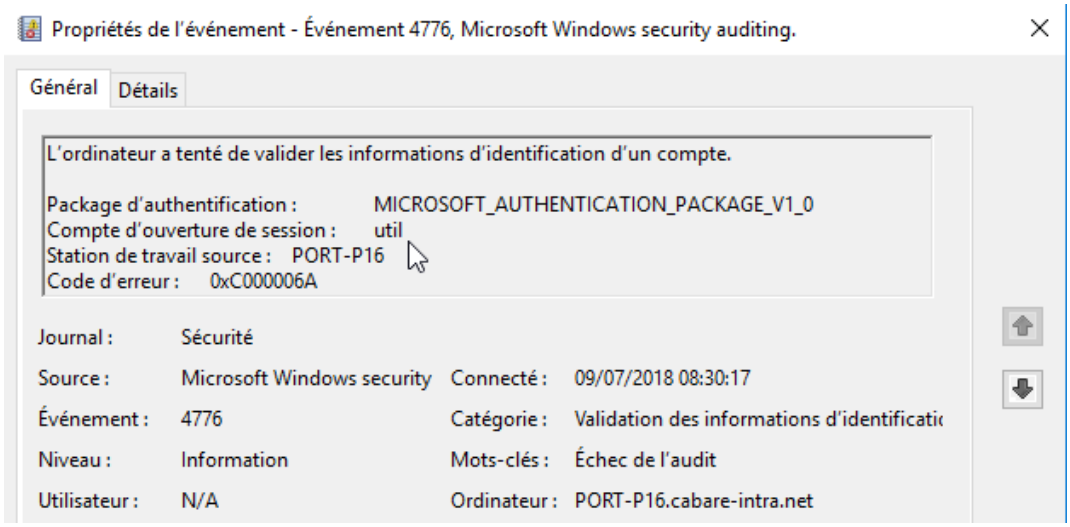
On va essayer d'ouvrir sur la machine une session locale avec une erreur de saisie du mot de passe… pour un utilisateur Existant local, par exemple ***util***



Une fois que l'erreur d'authentification a été commise, on se loggue en tant qu'administrateur, et on va voir notre journal (personnalisé ou non…)



Le détail montre que l'on a tenté de se loguer en tant que ***util***

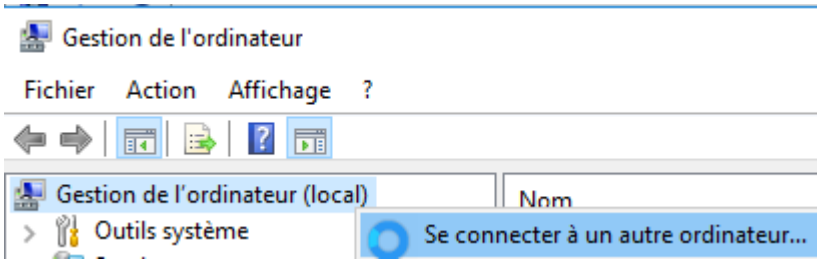


LOCALISATION DES EVENEMENTS

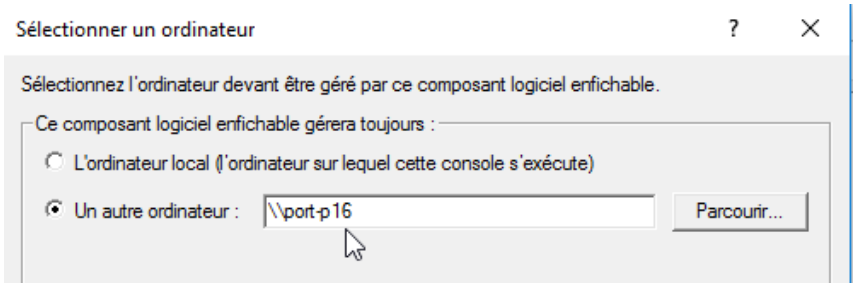
Localisation des Journaux d'évènement

La règle veut que les journaux soient consignés sur la machine sur laquelle l'évènement s'est produit.

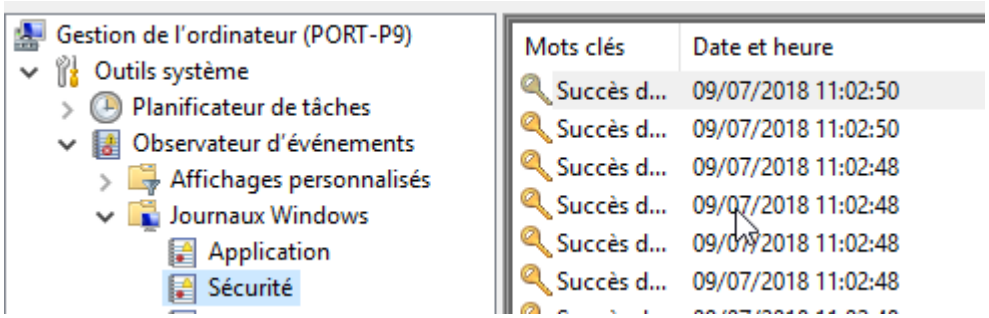
Pour afficher le journal d'un autre ordinateur, cliquez avec le bouton droit sur Gestion de l'ordinateur (local). Sélectionner **Se connecter à un autre ordinateur**



puis renseigner les champs de la boîte de dialogue



Il suffit ensuite d'aller chercher simplement l'observateur d'évènement



Il est cependant possible de les déporter de manière automatique sur une autre machine, pour faciliter leur lecture. Cela necéssite une opération en 3 étapes :

- Configuration des **clients collectés : WinRm + Compte ordi dans grp Admins + service reseau dans groupe lecteur journaux evenement +**
- Configuration du **poste collecteur :**
- Choix des évènements à colleter à travers un **abonnement**

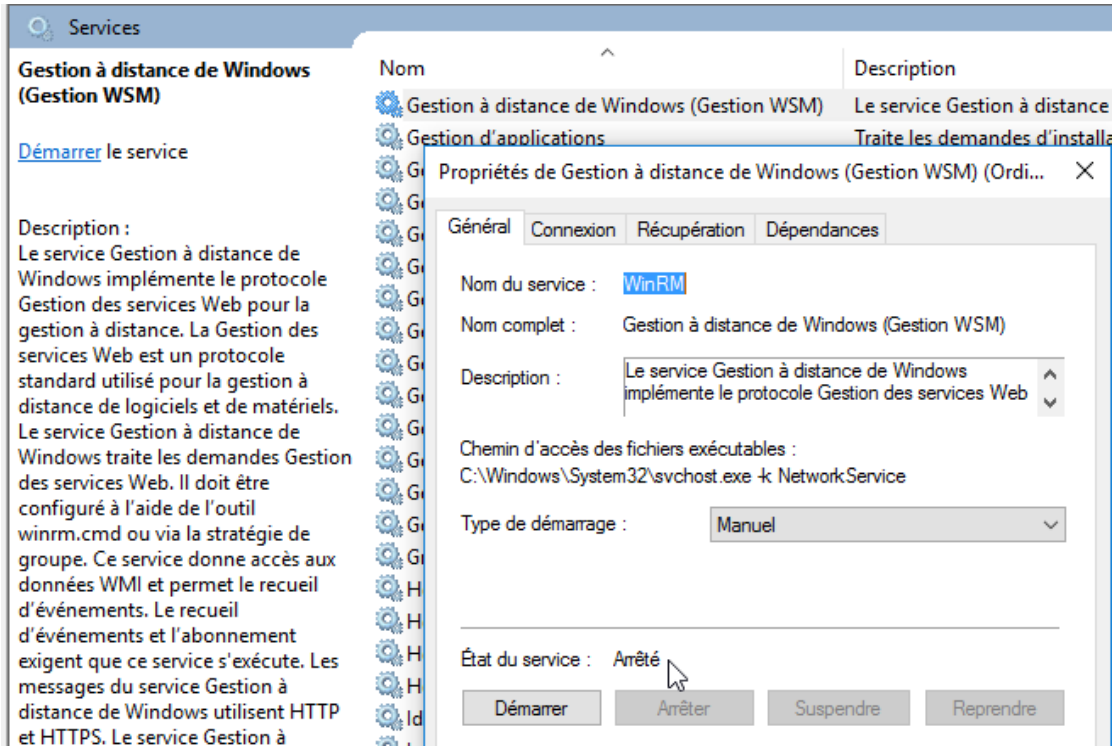
Configuration du client Collecté – WinRm – compte ordi

Il faut pour qu'un client soit collecté (collectable) activer le service spécifique **WinRm – Windows remote management** qui repose sur du http. C'est l'implémentation chez Microsoft du standard WS-Management, basé sur SOAP. Ceci implique qu'il n'est plus un protocole RPC et peut donc passer plus facilement les firewalls. Au niveau des ports utilisés, on en trouve deux :

HTTP : 5985 HTTPS : 5986

Un **sc query type= service state= all** donnerait

```
SERVICE_NAME: WinRM
DISPLAY_NAME: Gestion à distance de Windows (Gestion WSM)
        TYPE               : 20  WIN32_SHARE_PROCESS
        STATE              : 1  STOPPED
        WIN32_EXIT_CODE    : 1077  (0x435)
        SERVICE_EXIT_CODE  : 0  (0x0)
```



Windows Remote Management propose en standard plusieurs scripts d'administration, dont une configuration simplifiée. Avec un compte administrateur local, La commande

winrm quickconfig

déroule un petit assistant qui propose de mettre le service en mode automatique

```
C:\Windows\system32>winrm quickconfig
WinRM n'est pas configuré pour recevoir des demandes sur cet ordinateur.
Les modifications suivantes doivent être effectuées :

Démarrez le service WinRM.
Affectez un démarrage automatique à retardement au service WinRM.

Effectuer ces modifications [y/n] ? y
```

On répond **y** et on enchaine

```
WinRM a été mis à jour pour recevoir des demandes.

Le type du service WinRM a été correctement modifié.
Le service WinRM a démarré.
WinRM n'est pas configuré pour la gestion à distance de cet ordinateur.
Les modifications suivantes doivent être effectuées :

Créez un écouteur WinRM sur HTTP://* pour accepter les demandes de la gestion
P de cet ordinateur.
Activez l'exception de pare-feu WinRM.

Effectuer ces modifications [y/n] ? y
```

L'utilitaire propose d''écouter les demandes entrantes, et de configurer le pare-feu, On répond **y** et on enchaine

```
WinRM a été mis à jour pour la gestion à distance.

Écouteur WinRM créé sur HTTP://* pour accepter les demandes de la gestion de
 cet ordinateur.
Exception de pare-feu WinRM activée.
C:\Windows\system32>
```

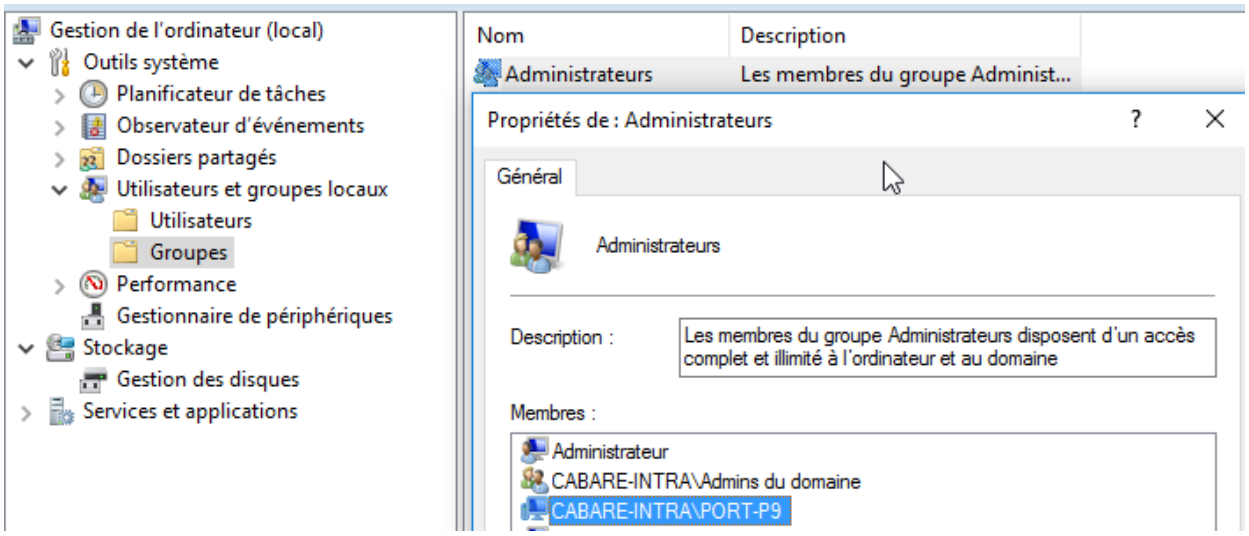
Cela peut aussi se faire en **Powershell** par la commande

Enable-psremoting

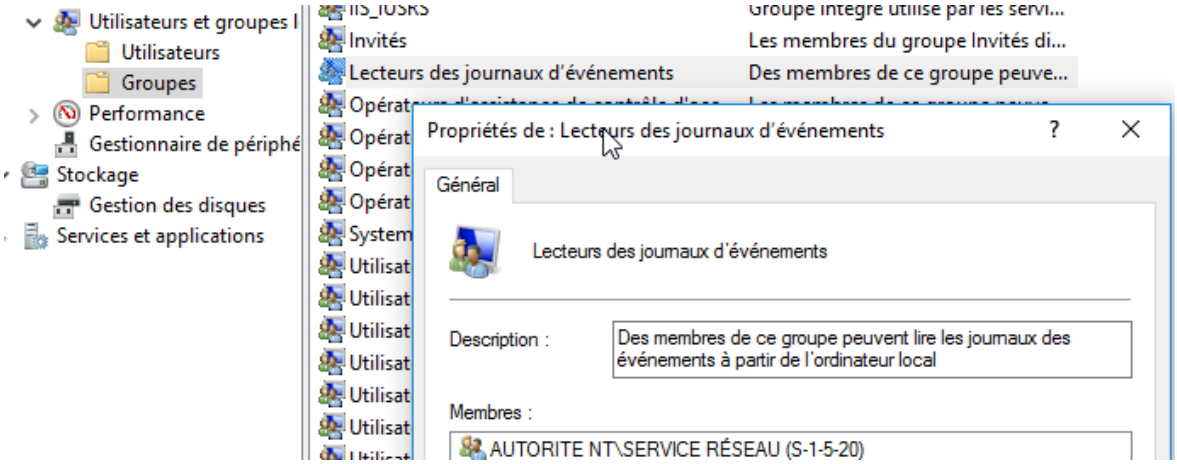
```
PS C:\Windows\system32> Enable-psremoting
WinRM a été mis à jour pour recevoir des demandes.
Le service WinRM a démarré.

WinRM est déjà configuré pour la gestion à distance sur cet ordinateur.
```

Il faut ajouter le **compte ordinateur** de la machine qui va collecter les évènements dans le groupe des **administrateurs locaux** de la machine auditée/collectée. Par exemple sur notre machine, sur laquelle on positionne l'audit, on veut envoyer nos évènement sur le poste collecteur distant ***port-p9***

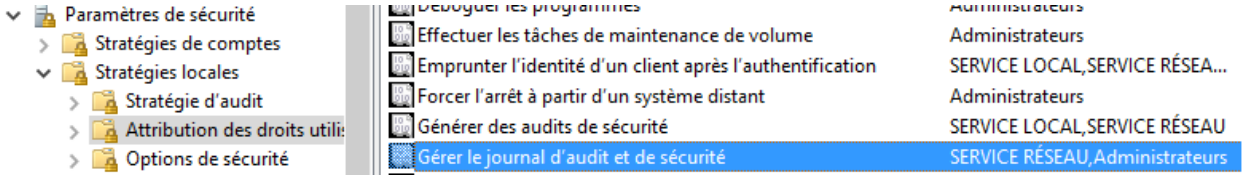
Il faut donc ajouter dans le groupe des administrateurs locaux de la machine auditée le compte machine vers laquelle on va exporter les journaux



Il faut ajouter le **service réseau** dans le groupe des **Lecteurs des journaux d'évènement** de la machine auditée/collectée.



Pour faire bon poids on peut aussi dans les **attributions des droits des Utilisateurs** on peut ajouter/vérifier que le Servive Réseau soit dans **Gérer le journal d'audit** et **générer des audits de sécurité**

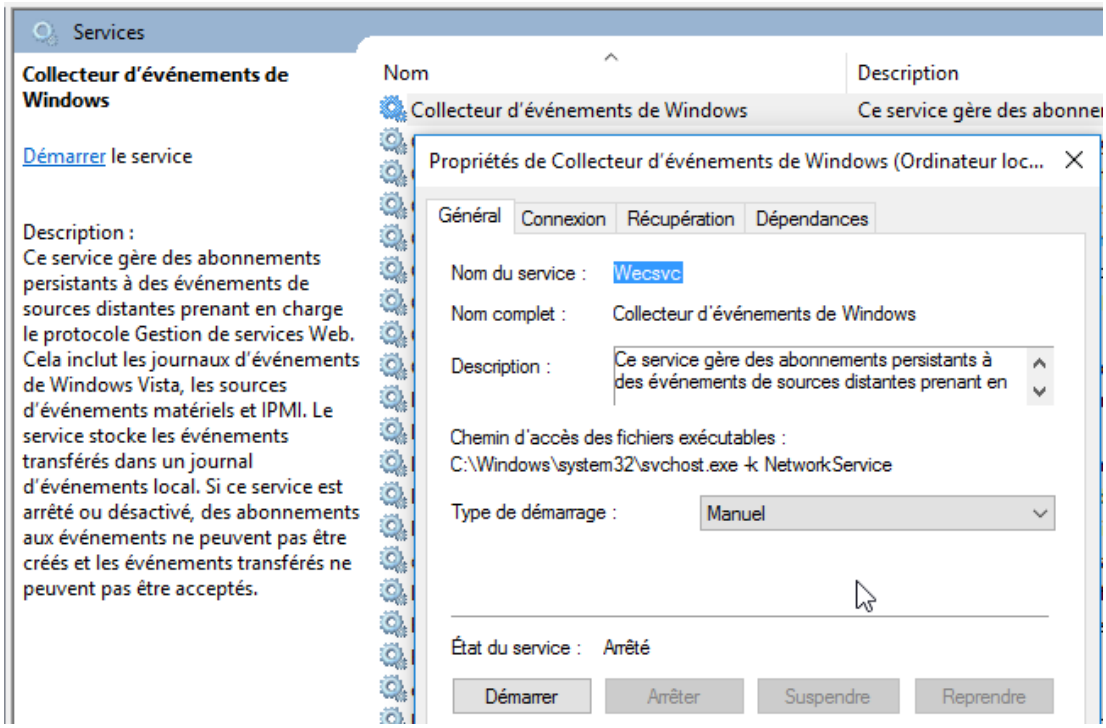


Configuration du poste Collecteur

Il faut activer le service **Windows Event collector.**

Un **sc query type= service state= all** donnerait

```
SERVICE_NAME: Wecsvc
DISPLAY_NAME: Collecteur d'événements de Windows
        TYPE               : 20  WIN32_SHARE_PROCESS
        STATE              : 1  STOPPED
```



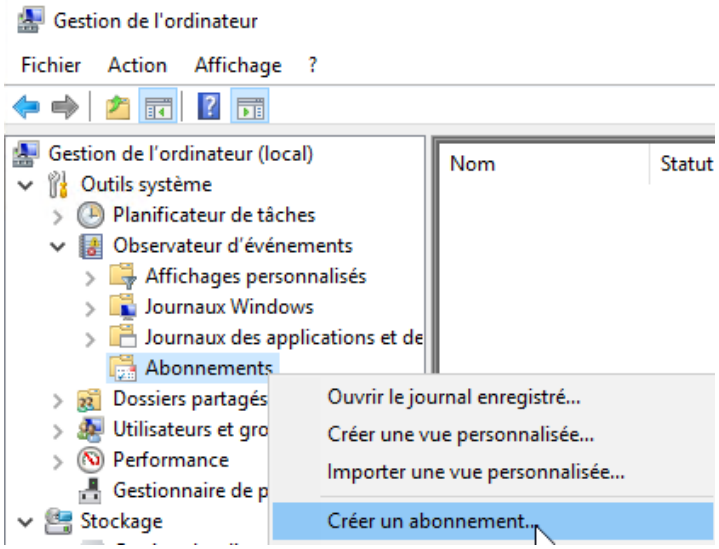
L'activation peut se faire avec une commande

Wecutil qc

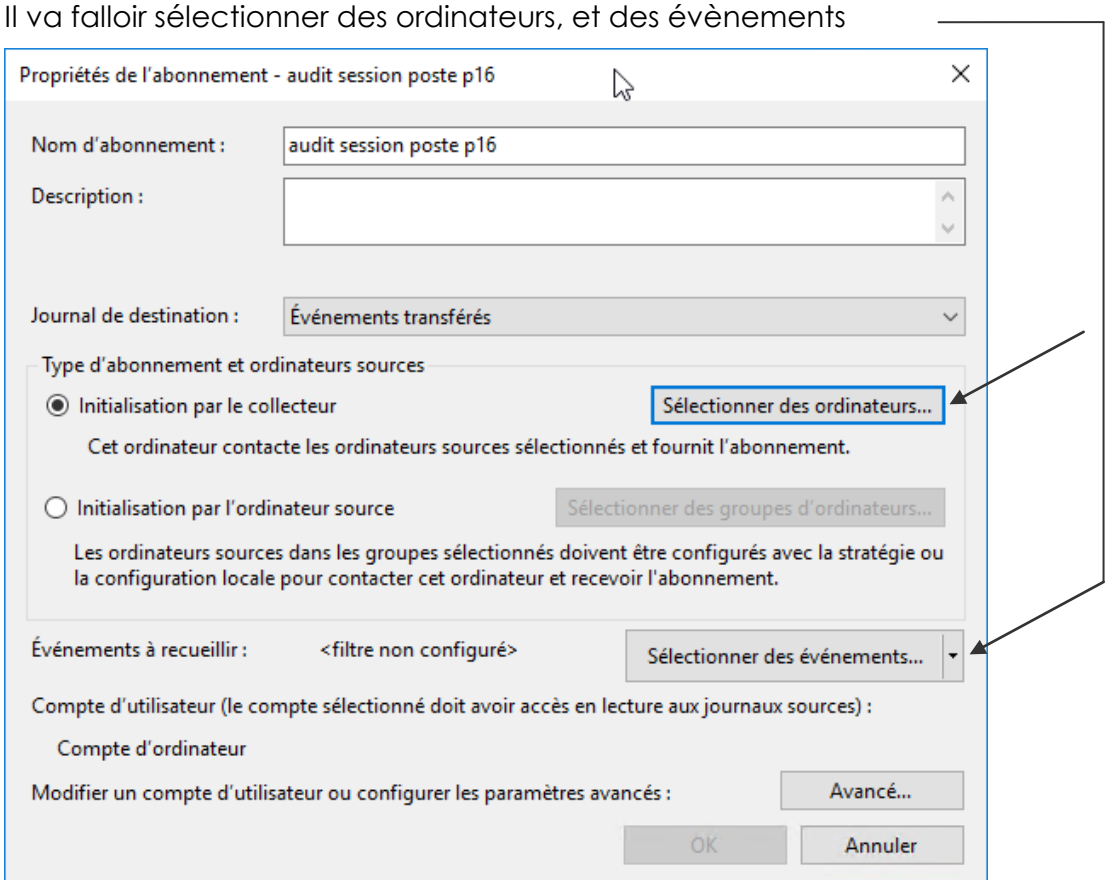
```
C:\Users\Administrateur>wecutil qc
Le mode de démarrage du service sera remplacé par Delay-Start. Voulez-vous continuer (O- oui ou N- non) ?o
Le service Collecteur d'événements Windows a été configuré.
```

Choix des évènements - abonnement

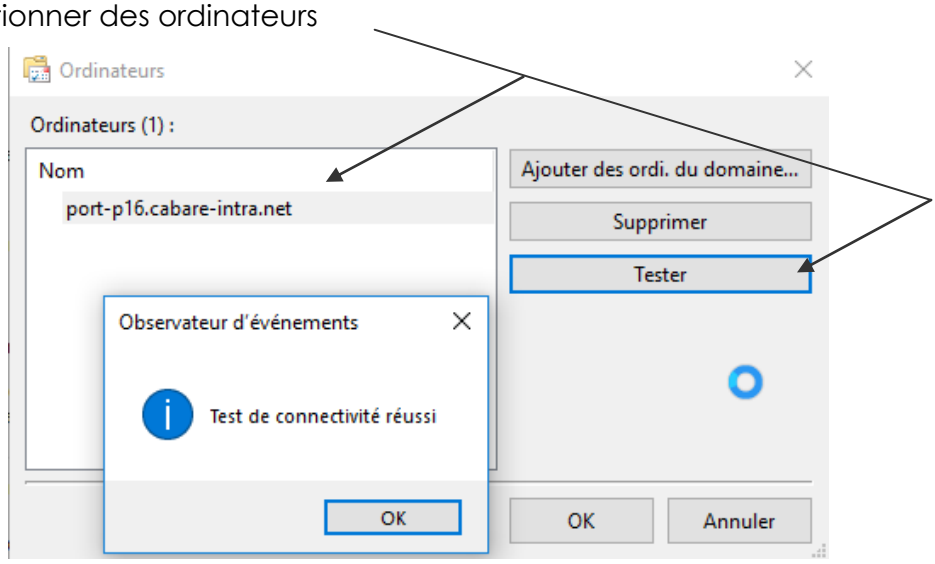
Sur l'ordinateur Collecteur, il faut maintenant indiquer ce que l'on souhaite recevoir. Cela se passe dans **l'observateur d'évènement**, (sur l'ordinateur collecteur) dans lequel on va dans **Abonnements, demander Créer un abonnement**



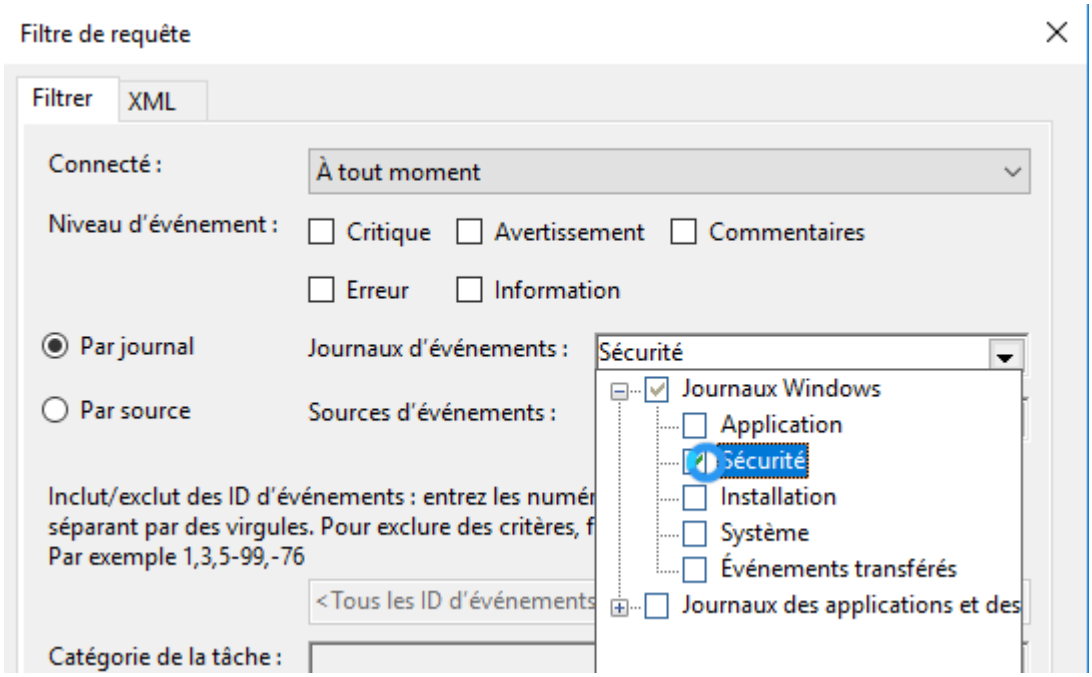
Il va falloir sélectionner des ordinateurs, et des évènements



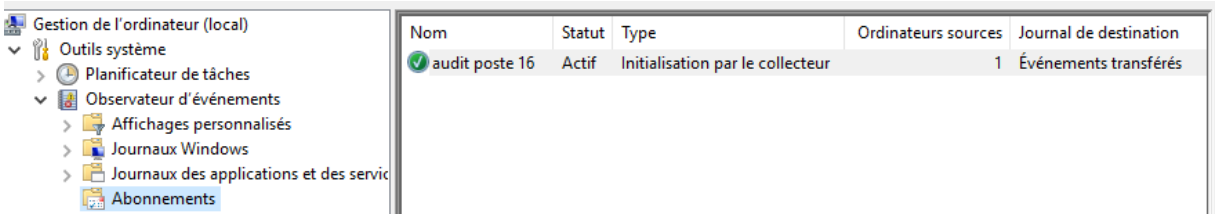
Sélectionner des ordinateurs



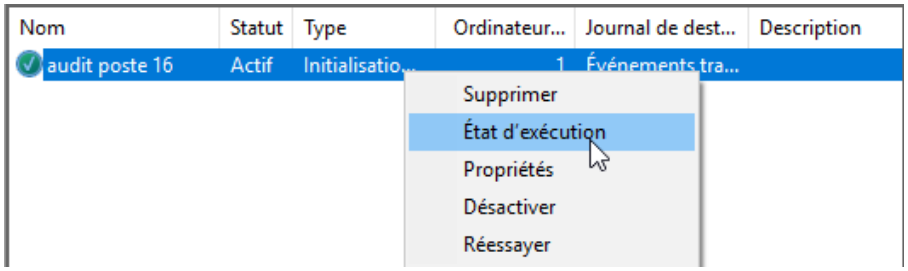
et faire un filtre de requête

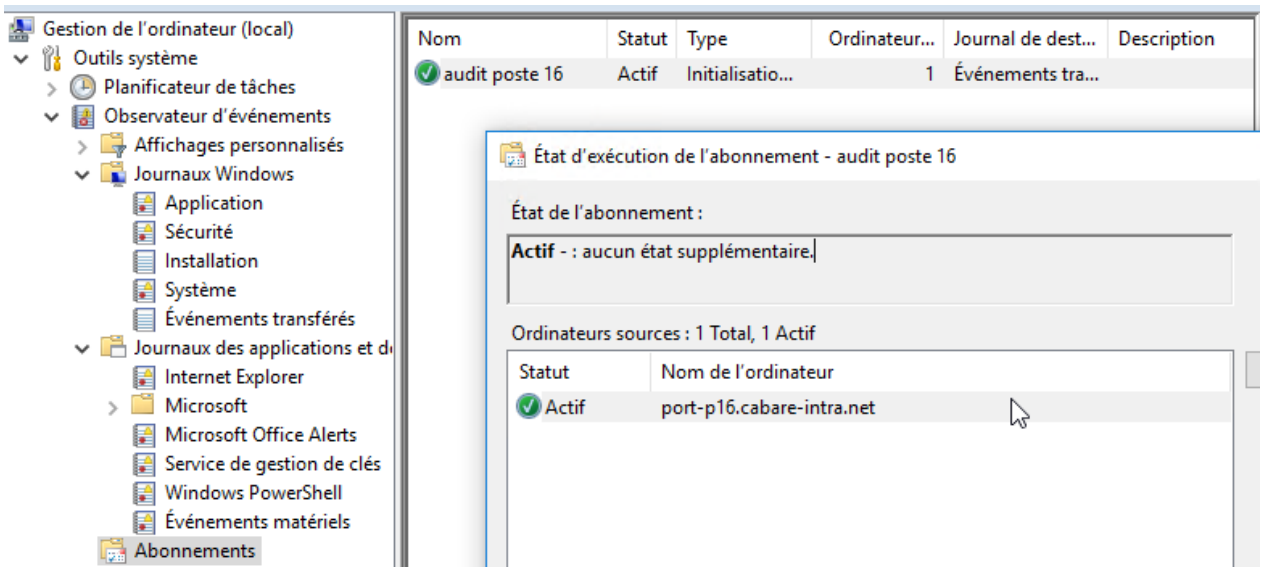


Et doit obtenir

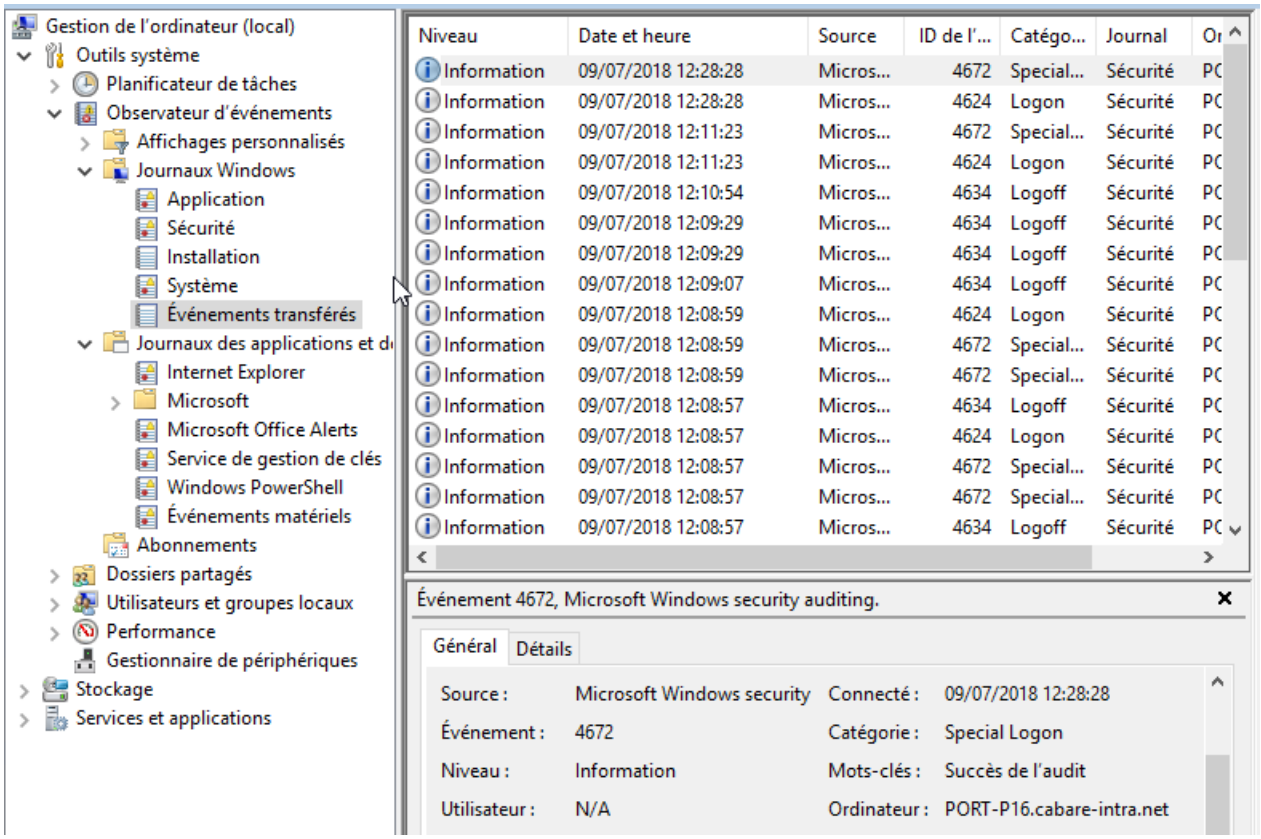


On peut via clic droit





Avec la possibiltité de vérifier que dans le journal **Evènement trasférés**, on a en fait les evènment de la machine collctée ***port-p16***



CONFIGURATION AVANCEE AUDIT

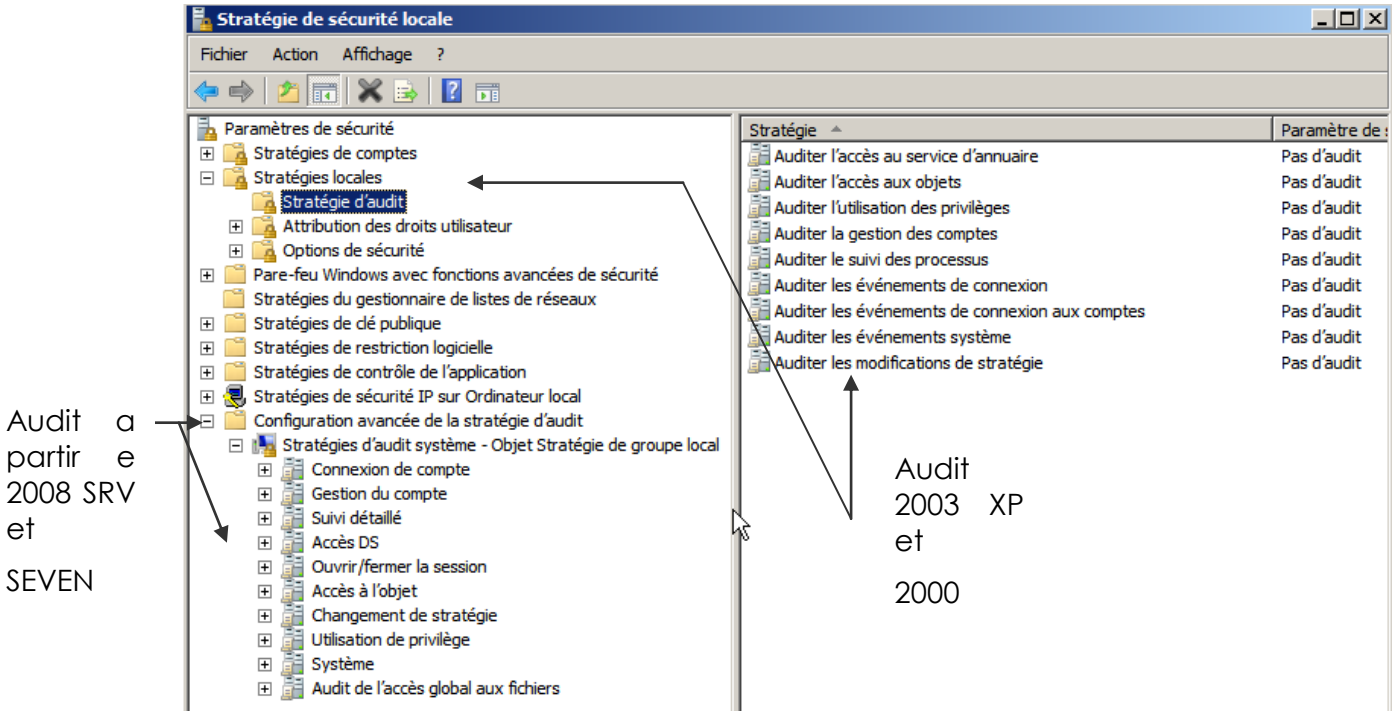
Configuration avancée de stratégies d'audit 10 - 7

Face à la verbosité des évènements de base, depuis SEVEN et Serveur 2008 on a rajouté des options complémentaires augmentant selon Microsoft la granularité de l'Audit. Permettant de ne plus activer les 9 niveaux ou catégories d'audit de base, mais on détaille plus de 53 réglages…

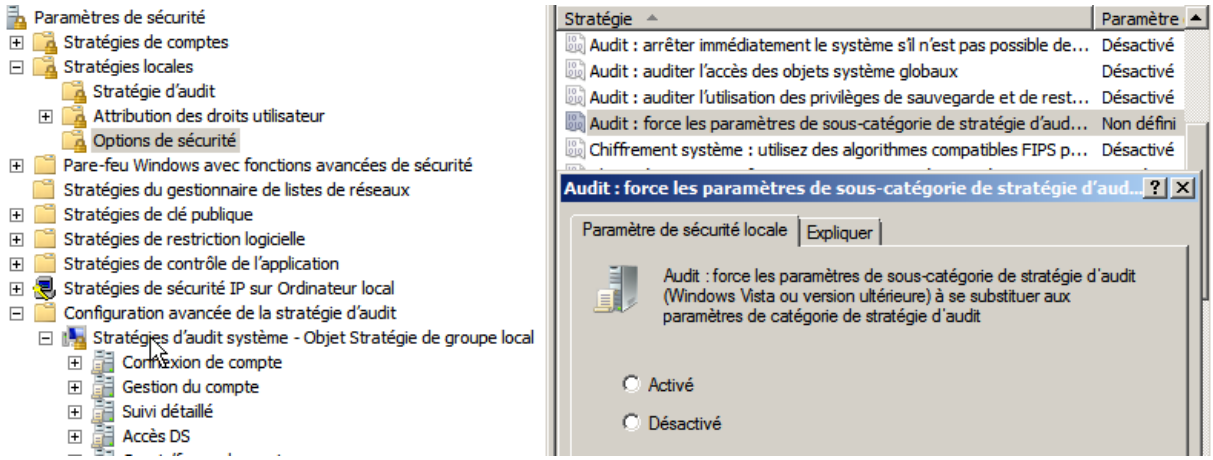
Le problème c'est que ces deux options

- **Stratégies d'audit** : sour XP 2000 et 2003
- **Configuration avancée de stratégies d'audit** : depuis SEVEN et 2008R2

Sont déclarées incompatibles, et qu'il faut choisir son camp…



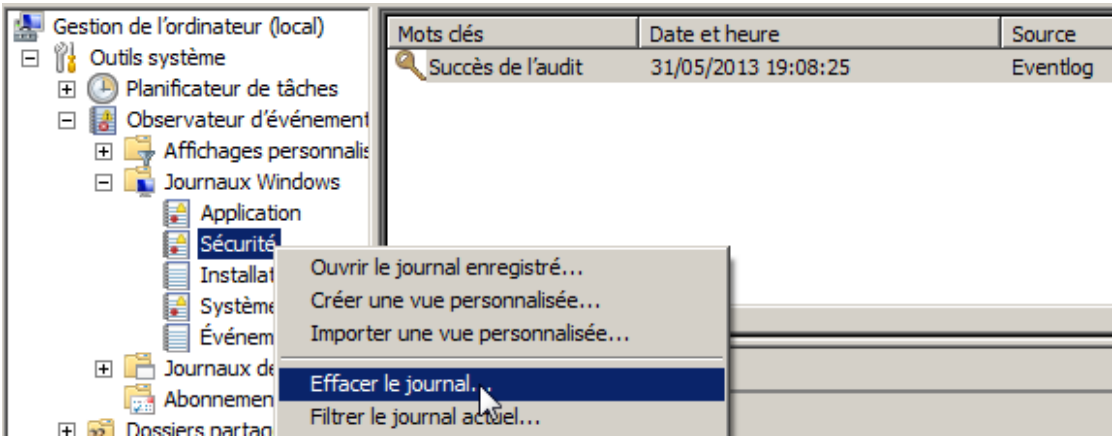
N.B : On <u>doit</u> indiquer via une stratégie **Options de Sécurité** si on veut que les nouvelles stratégies prennent le pas sur les anciennes



AuditPol - limites de l'interface graphique

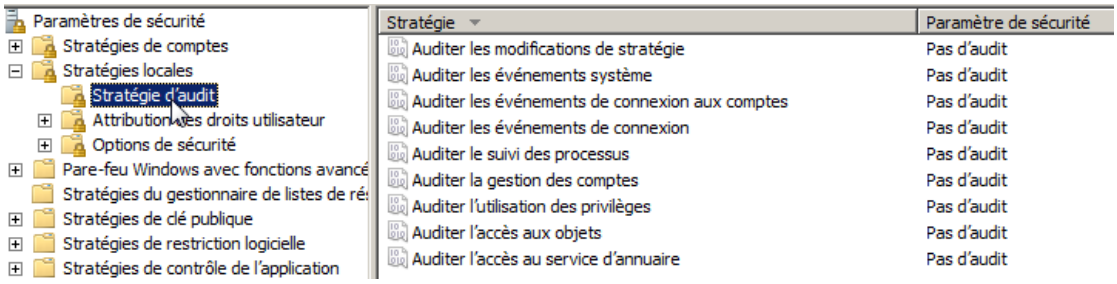
il existe des audits par défaut non visibles dans l'interface graphique...

effaçons le journal

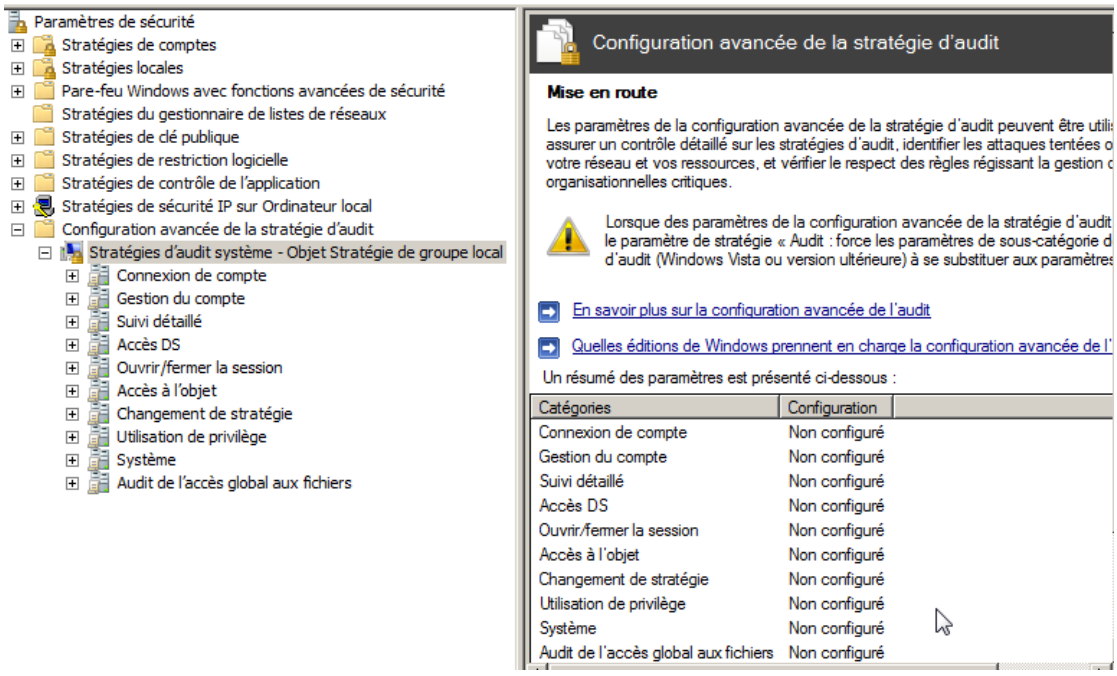


Vérifions qu'aucun audit n' est a priori armé en interface graphique..

ni standard par **Stratégie d'audit**



ni avancé par **Stratégies d'audit système**



et bien c'est faux !

redémarez le poste, et vérifier le journal d'évènements...

N.B vous ne pouvez pas gérer la stratégie d'audit au niveau sous-catégorie en utilisant les stratégies de groupe graphique.. il faut faire cela avec l'outils en invite de commande **auditpol**

Auditpol - Catégories et Sous catégories auditpol/list**:**

On peut lister les 10 catégories **auditpol/list /category**

```
C:\Users\Administrateur>auditpol/list /category
Catégorie/Sous-catégorie
Accès aux objets
Accès DS
Changement de stratégie
Connexion de compte
Gestion des comptes
Ouverture/Fermeture de session
Suivi détaillé
Système
Utilisation de privilège
```

On peut lister les sous catégorie par exemple

auditpol/list /subcategory:"système"

```
C:\Users\Administrateur>auditpol/list /subcategory:"système"
Catégorie/Sous-catégorie
Système
  Modification de l'état de la sécurité
  Extension système de sécurité
  Intégrité du système
  Pilote IPSEC
  Autres événements système
```

auditpol/list /subcategory:"Ouverture/Fermeture de session"

```
C:\Users\Administrateur>auditpol/list /subcategory:"Ouverture/Fermeture de sessi
on"
Catégorie/Sous-catégorie
Ouverture/Fermeture de session
  Ouvrir la session
  Fermer la session
  Verrouillage du compte
  Mode principal IPsec
  Mode rapide IPsec
  Mode étendu IPsec
  Ouverture de session spéciale
  Autres événements d'ouverture/fermeture de session
  Serveur NPS
```

Lister les audit auditpol/get**:**

lister tous les audits **auditpol/get /category :***

```
C:\Users\Administrateur>auditpol/get /category:*
Stratégie d'audit système
Catégorie/Sous-catégorie                    Paramètre
Système
  Extension système de sécurité             Aucun audit
  Intégrité du système                      Succès et échec
  Pilote IPSEC                              Aucun audit
  Autres événements système                 Succès et échec
  Modification de l'état de la sécurité     Opération réussie
Ouverture/Fermeture de session
  Ouvrir la session                         Succès et échec
  Fermer la session                         Opération réussie
  Verrouillage du compte                    Opération réussie
  Mode principal IPsec                      Aucun audit
  Mode rapide IPsec                         Aucun audit
```

On peut listes les audits en place par catégories

auditpol /get /Category:"système"

```
C:\Users\Administrateur>auditpol /get /Category:"système"
Stratégie d'audit système
Catégorie/Sous-catégorie                    Paramètre
Système
  Extension système de sécurité             Aucun audit
  Intégrité du système                      Succès et échec
  Pilote IPSEC                              Aucun audit
  Autres événements système                 Succès et échec
  Modification de l'état de la sécurité     Opération réussie
```

Par défaut

Et visualiser une par une

auditpol /get /SubCategory:"intégrité du système"

```
C:\Users\Administrateur>auditpol /get /SubCategory:"intégrité du système"
Stratégie d'audit système
Catégorie/Sous-catégorie                    Paramètre
Système
  Intégrité du système                      Succès et échec
```

Modifier les audit auditpol/set**:**

Et les modifier, globalement par catégories complète

auditpol /set /Category:"système" / failure:disable

```
C:\Users\Administrateur>auditpol /set /Category:"système" /failure:disable
Commande exécutée correctement.
```

Donnant (on a désactivé tous les audits en echec)

```
C:\Users\Administrateur>auditpol /get /Category:"système"
Stratégie d'audit système
Catégorie/Sous-catégorie                    Paramètre
Système
  Extension système de sécurité             Aucun audit
  Intégrité du système                      Opération réussie
  Pilote IPSEC                              Aucun audit
  Autres événements système                 Opération réussie
  Modification de l'état de la sécurité     Opération réussie
```

Et voilà la séquence désactivant aussi les audits en succès,

auditpol /set /Category:"système" / success:disable

```
C:\Users\Administrateur>auditpol /get /Category:"système"
Stratégie d'audit système
Catégorie/Sous-catégorie                    Paramètre
Système
  Extension système de sécurité             Aucun audit
  Intégrité du système                      Succès et échec
  Pilote IPSEC                              Aucun audit
  Autres événements système                 Succès et échec
  Modification de l'état de la sécurité     Opération réussie

C:\Users\Administrateur>auditpol /set /Category:"système" /failure:disable
Commande exécutée correctement.

C:\Users\Administrateur>auditpol /get /Category:"système"
Stratégie d'audit système
Catégorie/Sous-catégorie                    Paramètre
Système
  Extension système de sécurité             Aucun audit
  Intégrité du système                      Opération réussie
  Pilote IPSEC                              Aucun audit
  Autres événements système                 Opération réussie
  Modification de l'état de la sécurité     Opération réussie

C:\Users\Administrateur>auditpol /set /Category:"système" /success:disable
Commande exécutée correctement.

C:\Users\Administrateur>auditpol /get /Category:"système"
Stratégie d'audit système
Catégorie/Sous-catégorie                    Paramètre
Système
  Extension système de sécurité             Aucun audit
  Intégrité du système                      Aucun audit
  Pilote IPSEC                              Aucun audit
  Autres événements système                 Aucun audit
  Modification de l'état de la sécurité     Aucun audit
```

Après Reset

donc au final désactivant tous les audits système…

Désactiver tous les audits

il faut pour chaque catégorie la lister via

auditpol /get /category:"xxxxxxx"

et si besoin effectuer ensuite

auditpol /set /category:"xxxxxxx" /success:disable

auditpol /set /category:"xxxxxxx" /failure:disable

```
Système
  Extension système de sécurité             Aucun audit
  Intégrité du système                      Aucun audit
  Pilote IPSEC                              Aucun audit
  Autres événements système                 Aucun audit
  Modification de l'état de la sécurité     Aucun audit
```

```
Ouverture/Fermeture de session
  Ouvrir la session                          Aucun audit
  Fermer la session                          Aucun audit
  Verrouillage du compte                     Aucun audit
  Mode principal IPsec                       Aucun audit
  Mode rapide IPsec                          Aucun audit
  Mode étendu IPsec                          Aucun audit
  Ouverture de session spéciale              Aucun audit
  Autres événements d'ouverture/fermeture de sessionAucun audit
  Serveur NPS                                Aucun audit
```

```
Accès aux objets
  Système de fichiers                        Aucun audit
  Registre                                   Aucun audit
  Objet de noyau                             Aucun audit
  SAM                                        Aucun audit
  Services de certification                  Aucun audit
  Généré par application                     Aucun audit
  Manipulation de handle                     Aucun audit
  Partage de fichiers                        Aucun audit
  Rejet de paquet par la plateforme de filtrageAucun audit
  Connexion de la plateforme de filtrage     Aucun audit
  Autres événements d'accès à l'objet        Aucun audit
  Partage de fichiers détaillé               Aucun audit
```

```
Utilisation de privilège
  Utilisation de privilèges sensibles        Aucun audit
  Utilisation de privilèges non sensibles    Aucun audit
  Autres événements d'utilisation de privilègesAucun audit
```

```
Suivi détaillé
  Fin du processus                           Aucun audit
  Activité DPAPI                             Aucun audit
  Événements RPC                             Aucun audit
  Création du processus                      Aucun audit
```

```
Changement de stratégie
  Modification de la stratégie d'audit       Aucun audit
  Modification de la stratégie d'authentificationAucun audit
  Modification de la stratégie d'autorisationAucun audit
  Modification de la stratégie de niveau règle MPSSVCAucun audit
  Modification de la stratégie de plateforme de filtrageAucun audit
  Autres événements de modification de stratégieAucun audit
```

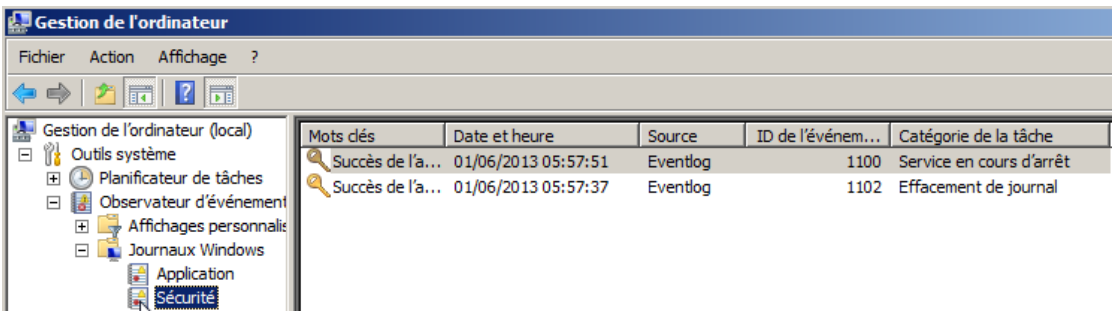
```
Gestion des comptes
  Gestion des comptes d'utilisateur          Aucun audit
  Gestion des comptes d'ordinateur           Aucun audit
  Gestion des groupes de sécurité            Aucun audit
  Gestion des groupes de distribution        Aucun audit
  Gestion des groupes d'applications         Aucun audit
  Autres événements de gestion des comptesAucun audit
```

```
Accès DS
  Modification du service d'annuaire         Aucun audit
  Réplication du service d'annuaire          Aucun audit
  Réplication du service d'annuaire détailléAucun audit
  Accès au service d'annuaire                Aucun audit
```

```
Connexion de compte
  Opérations de ticket du service KerberosAucun audit
  Autres événements d'ouverture de sessionAucun audit
  Service d'authentification Kerberos        Aucun audit
  Validation des informations d'identificationAucun audit
```

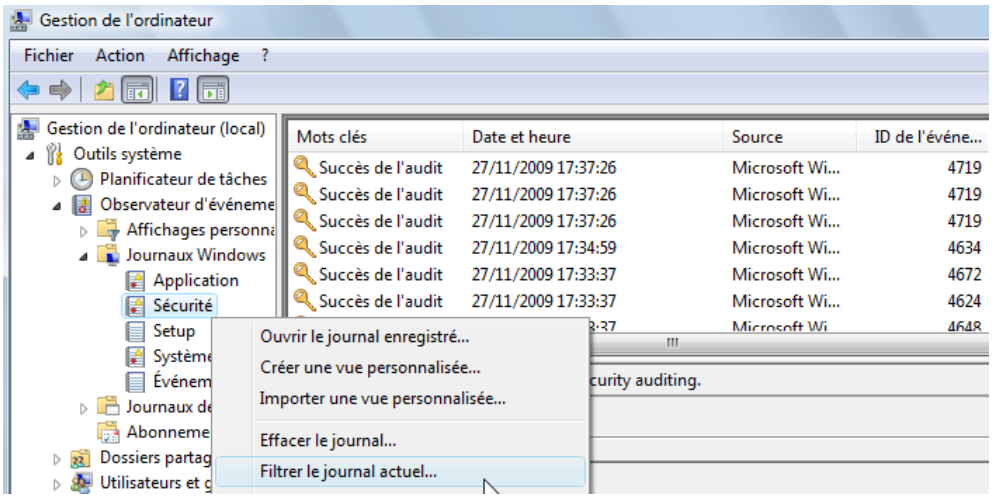
Et que l'on efface ensuite le journal…

Lors d'un re-démarage, les événements sont réduits au minimum...

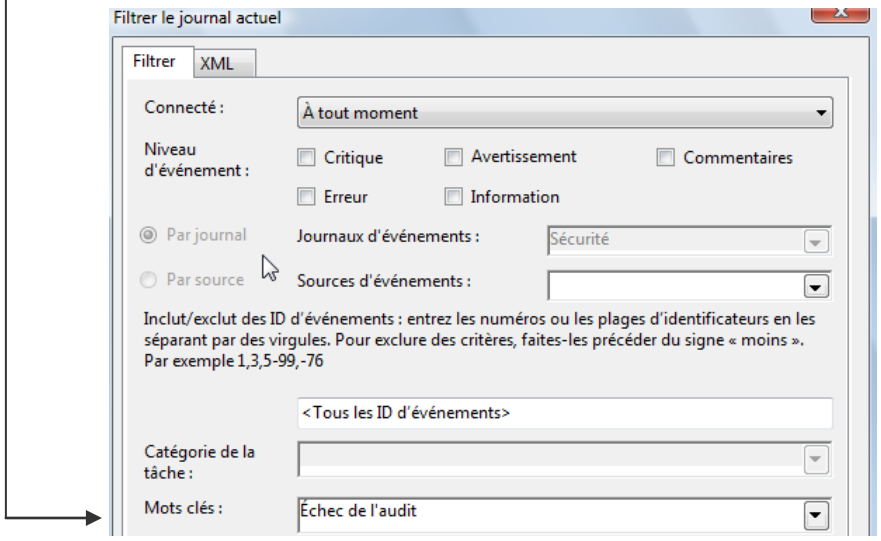


Lire le journal de sécurité:

les évènements de sécurité sont consignés dans le journal d'événement **Journaux Windows / Sécurité**. pour s'aider on peut le filtrer…



Dans lequel on peut indiquer par exemple dans notre cas



Installer un Audit sur des ressources:

Lorsque l'on souhaite installer un **Audit sur des ressources**, l'opération se fait en deux temps. En effet il ne suffit pas de demander d'activer l'audit sur telle ou telle type d'événement (comme cela était le cas pour les session, ou les identification du chapitre précédant), mais il va falloir aussi activer l'audit sur les ressources que l'on veut observer…Il faut donc :

1. activer le type d'audit souhaité, c'est à dire Audit "**Accès aux objets**"dans les stratégies locales de l'ordinateur
2. activer ensuite "**pour chaque ressource**" l'audit particulier (en plus de la sécurité d'accès éventuellement posée

Audit ressource sur un dossier

Il faut

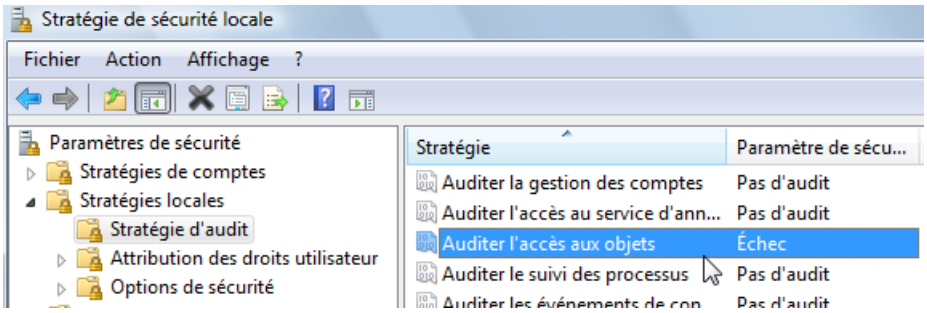
1. activer l' Audit "**Accès aux objets**" dans les stratégies locales de l'ordinateur sur lequel le dossier est stocké

2. sur ce dossier ensuite, il faut demander les **propriétés**, onglet **sécurité**, via les **Paramètres avancées NTFS** et demander **Audit** …

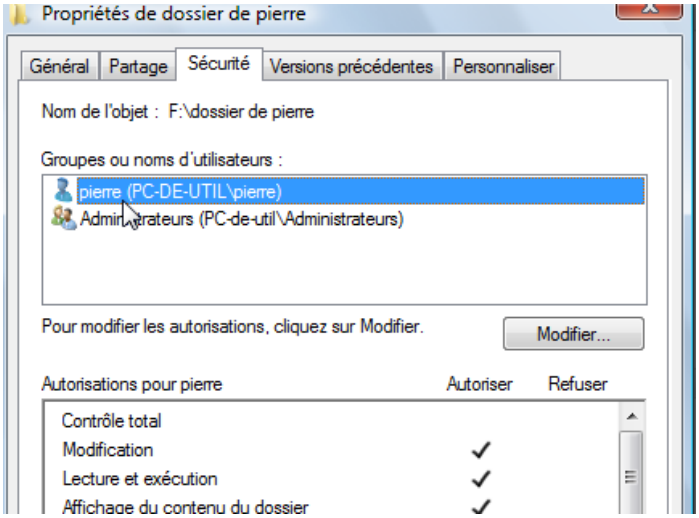
Exemple :

On veut un audit sur les accès en échec pour le dossier de pierre (on cherche à savoir qui essaye d'effacer le dossier de pierre…)

1. Il faut armer les **audits en Echec** sur le poste



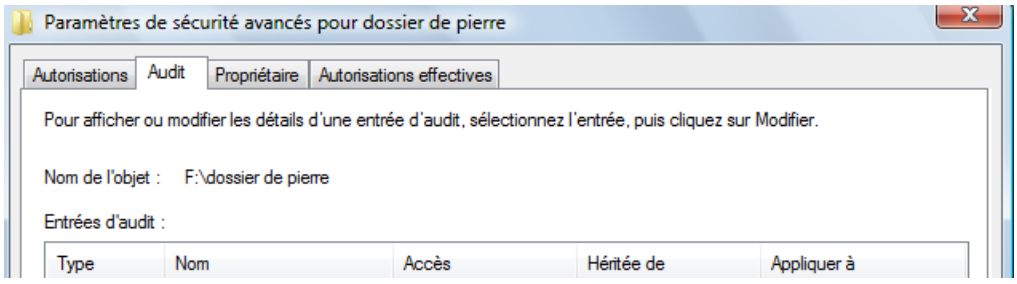
2. Il faut que le dossier de pierre soit protégé en NTFS, bien sûr…



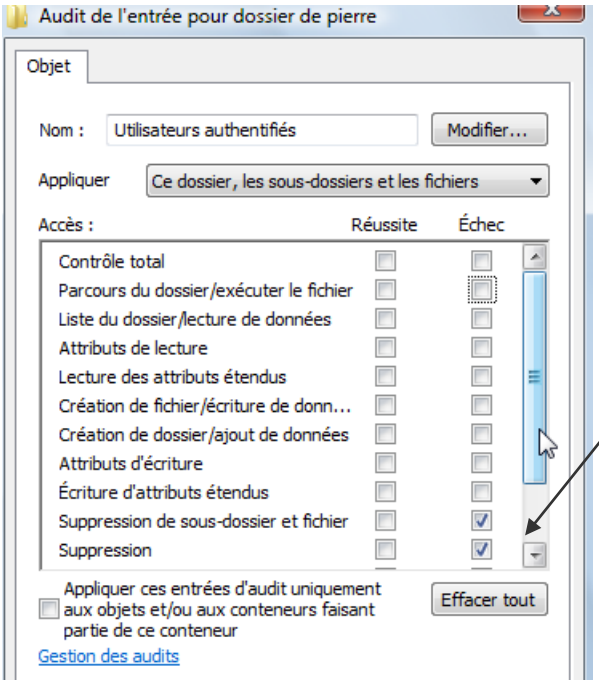
3. puis que l'on pose un audit dessus

via l'onglet **sécurité / avancé** des **propriétés** ce dossier de pierre…

on accès à la boite de dialogue **Paramètre de sécurité avancé pour...**



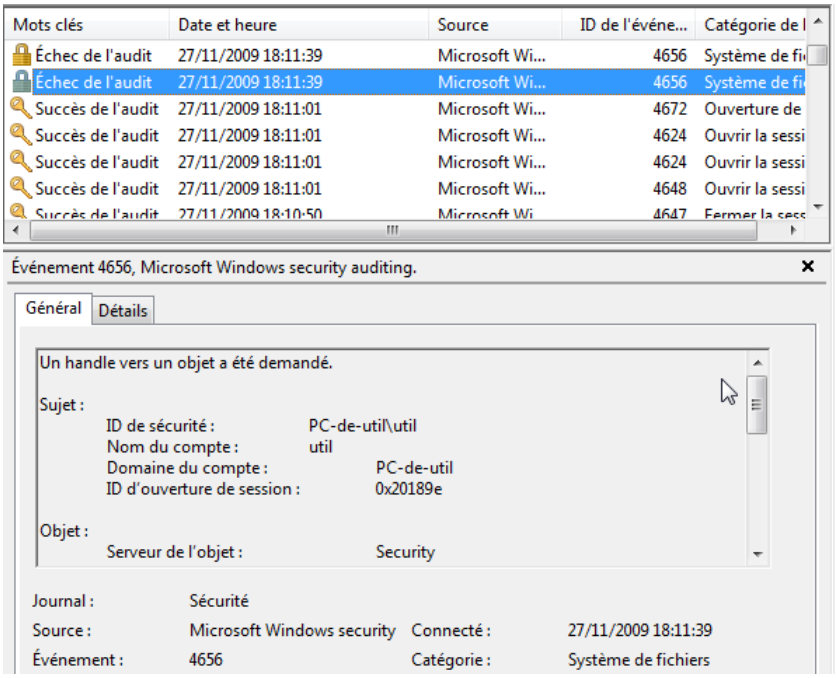
Il faut ensuite ajouter pour qui et quel type d'Audit l'on veut correspondant à



Les types d'audit en tentative de suppression peuvent être obtenus par **Suppression**

N.B : Ne pas cocher tous les accès car cela génère autant d'évènements de plus !!!

Lorsque ensuite un utilisateur tiers essaye d'effacer le dossier, cela sera tracé…

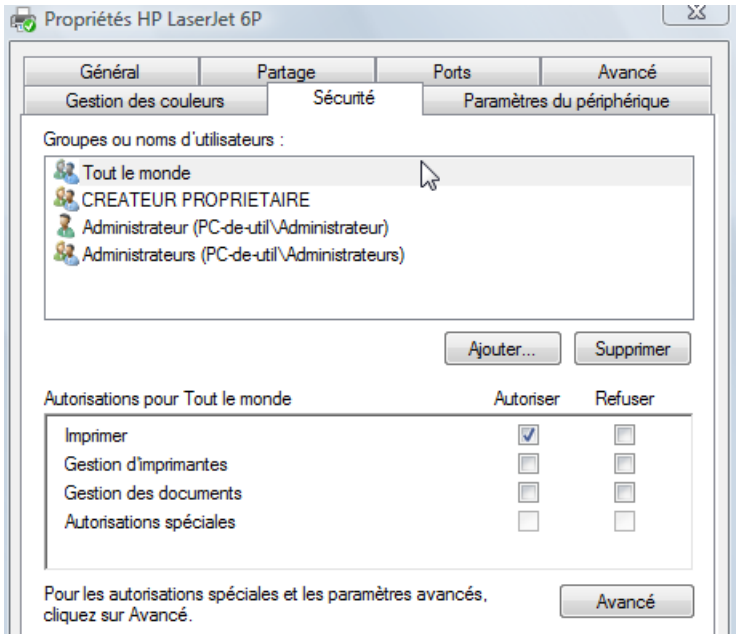


Audit ressource sur une imprimante

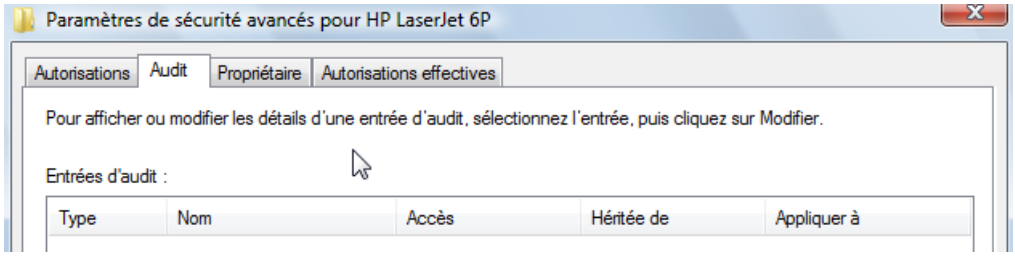
On veut savoir qui utilise l'imprimante réellement :

Il faut

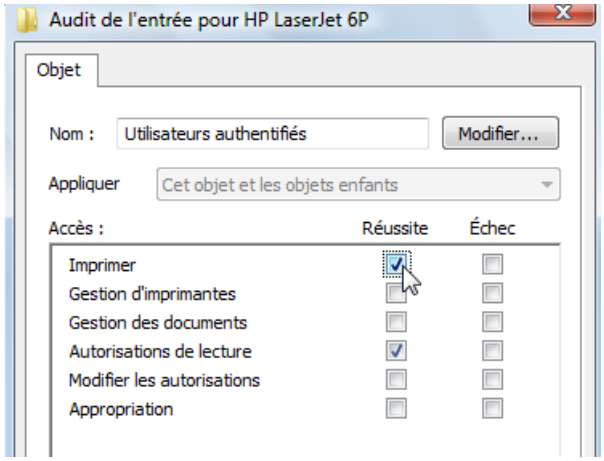
1. activer l' Audit "**Accès aux objets**" en succès dans les stratégies locales de l'ordinateur sur lequel l'imprimante est connectée…
2. sur cette imprimante demander par les **Propriétés avancées NTFS** onglet **Sécurité**, puis bouton Avancé



3. on accès à la boite de dialogue **Paramètre de sécurité avancé pour...**



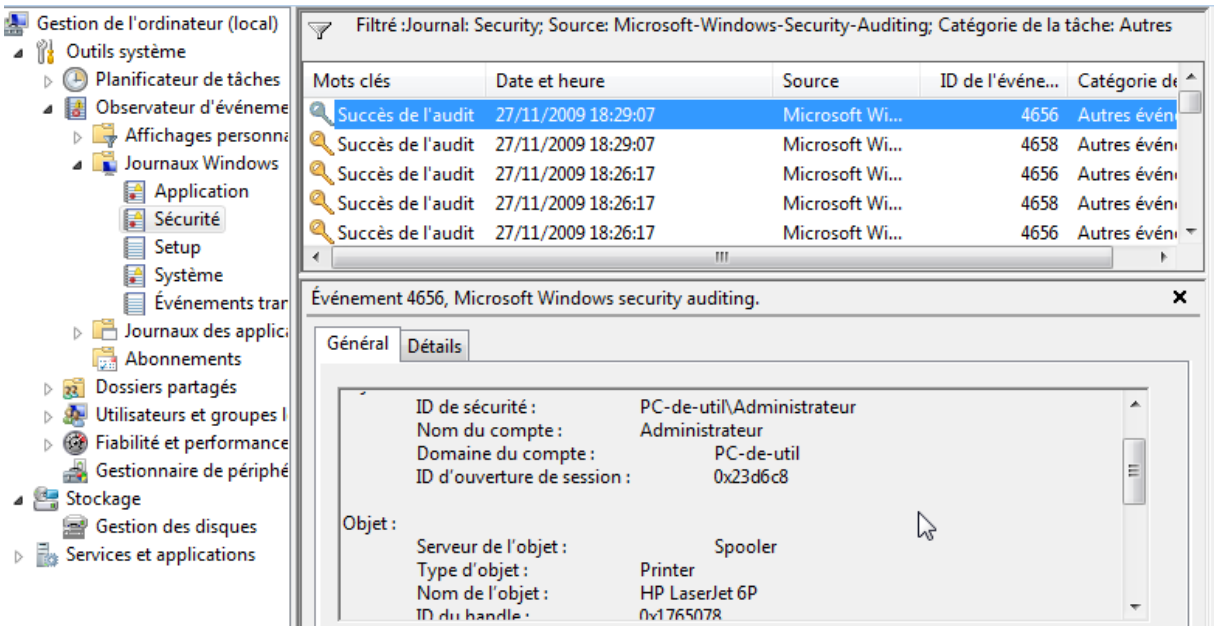
Et il faut indiquer ce que l'on veut auditer



Les types d'audit en tentative 'impression » peuvent être obtenu par **Imprimer**

N.B : Ne pas cocher tous les accès car cela génère autant d'évènements de plus !!!

Ensuite il faut après une impression voir le journal d'évènements…


Gestion de l'ordinateur (local)
Outils système
Planificateur de tâches
Observateur d'événeme
Affichages personna
Journaux Windows
Application
Sécurité
Setup
Système
Événements trar
Journaux des applic
Abonnements
Dossiers partagés
Utilisateurs et groupes l
Fiabilité et performance
Gestionnaire de périphé
Stockage
Gestion des disques
Services et applications
Filtré :Journal: Security; Source: Microsoft-Windows-Security-Auditing; Catégorie de la tâche: Autres
Mots clés
Date et heure
Source
ID de l'événe...
Catégorie de
Succès de l'audit 27/11/2009 18:29:07 Microsoft Wi... 4656 Autres évén
Succès de l'audit 27/11/2009 18:29:07 Microsoft Wi... 4658 Autres évén
Succès de l'audit 27/11/2009 18:26:17 Microsoft Wi... 4656 Autres évén
Succès de l'audit 27/11/2009 18:26:17 Microsoft Wi... 4658 Autres évén
Succès de l'audit 27/11/2009 18:26:17 Microsoft Wi... 4656 Autres évén
Événement 4656, Microsoft Windows security auditing.
Général
Détails
ID de sécurité : PC-de-util\Administrateur
Nom du compte : Administrateur
Domaine du compte : PC-de-util
ID d'ouverture de session : 0x23d6c8
Objet :
Serveur de l'objet : Spooler
Type d'objet : Printer
Nom de l'objet : HP LaserJet 6P
ID du handle : 0x1765078

STRATEGIE AUDIT EVENEMENT

Pister les tentatives d'accès :

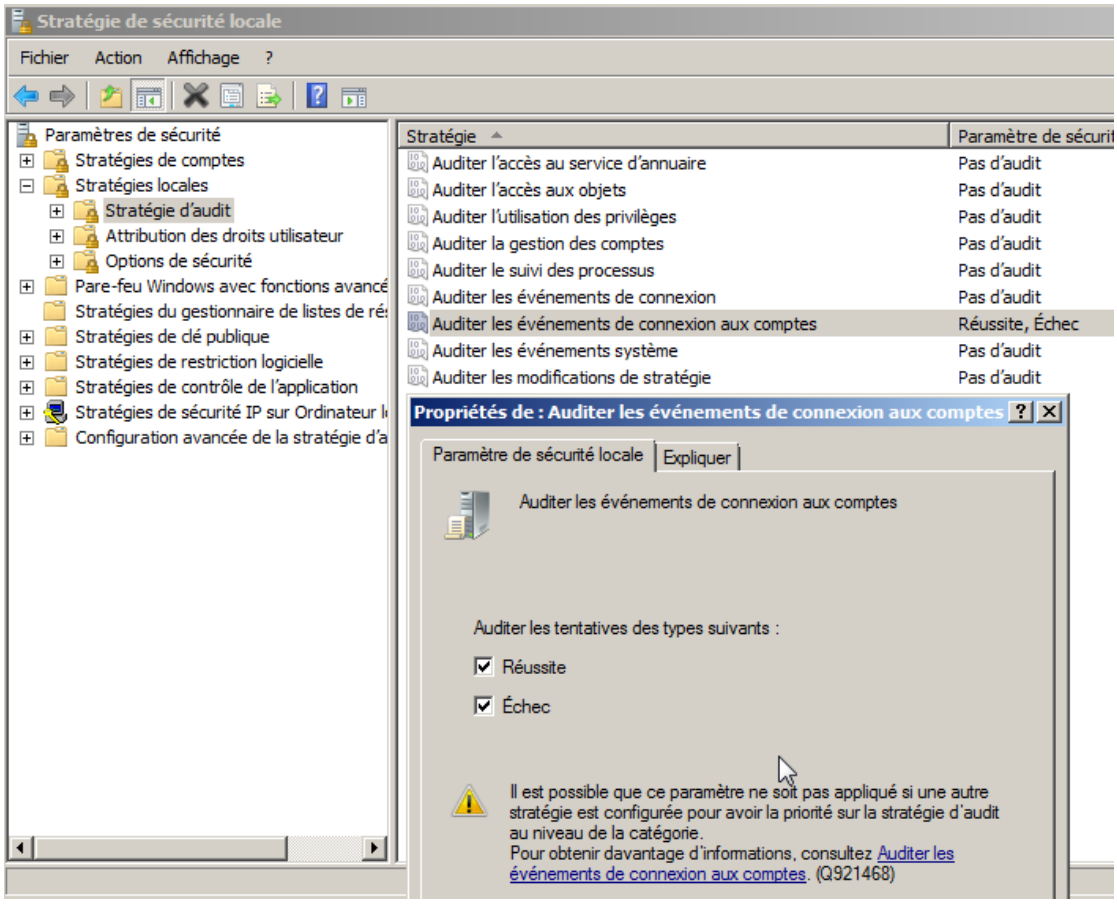
Le principe va consister à armer une stratégie d'audit basée sur les **évènements de connexion aux comptes**.

Par définition on n'auditera que les tentatives qui échouent, en sachant que l'événement est enregistré sur la machine sur laquelle l'identification se fera…

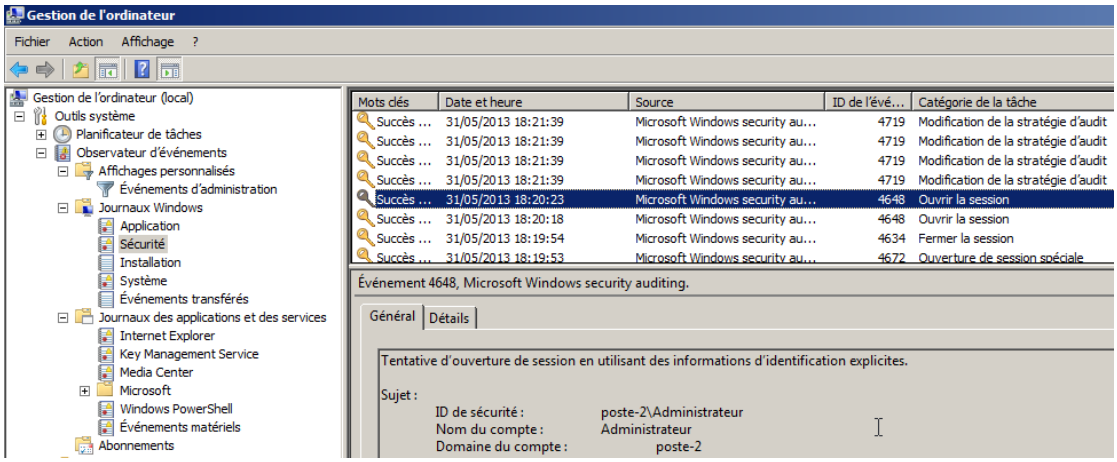
Audit évènement connexion aux comptes sur un client 7 :

On suppose que les tentatives de connexions se font depuis une machine isolée dans un bâtiment, la nuit....

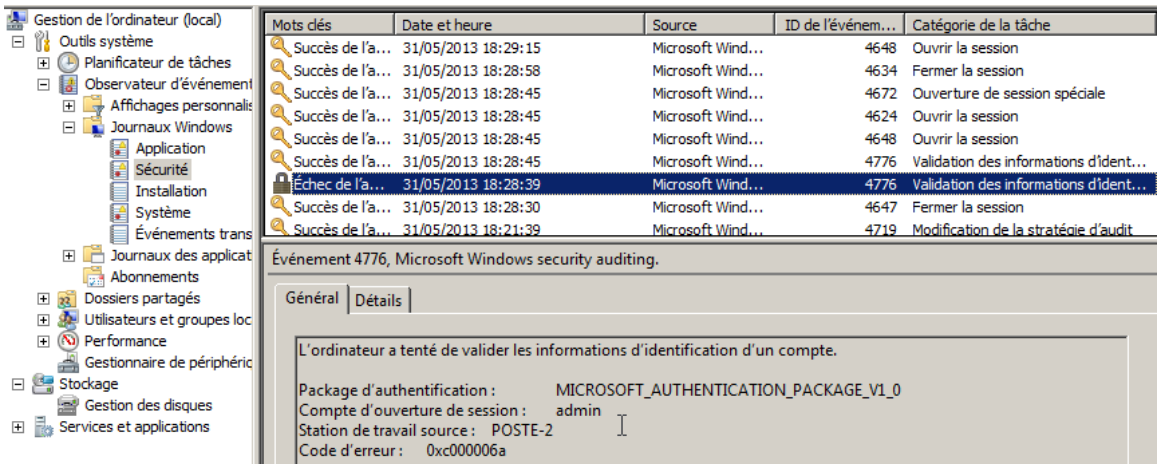
On va placer dessus donc un **audit sur les réussites et les echec**.



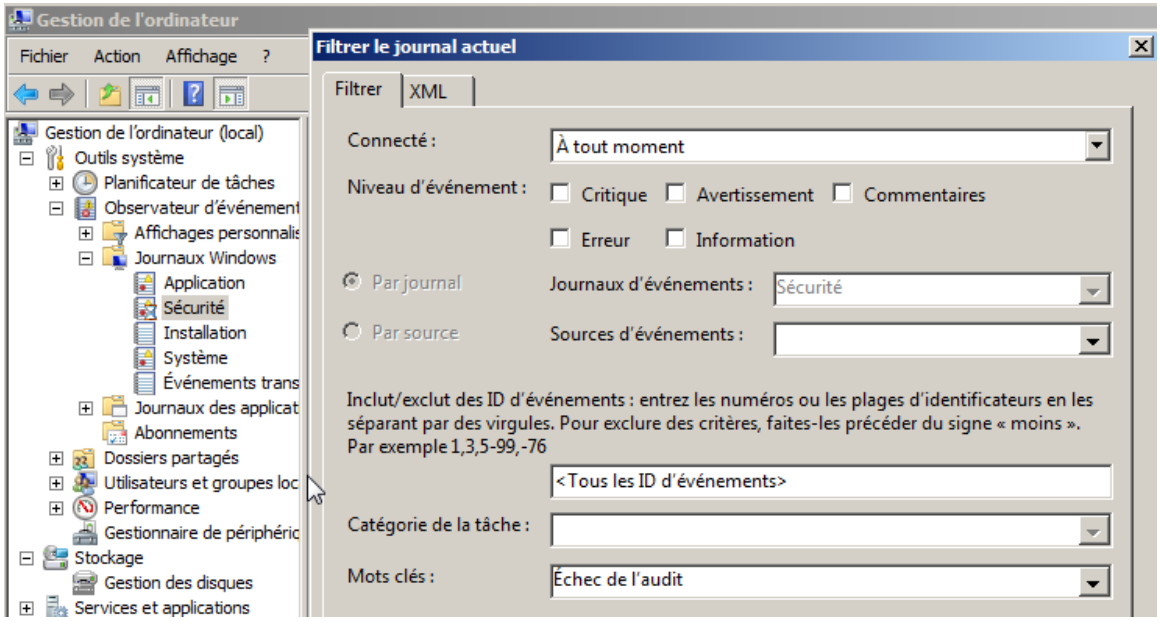
pour l'instant dans l'observateur d'evenement on trouve



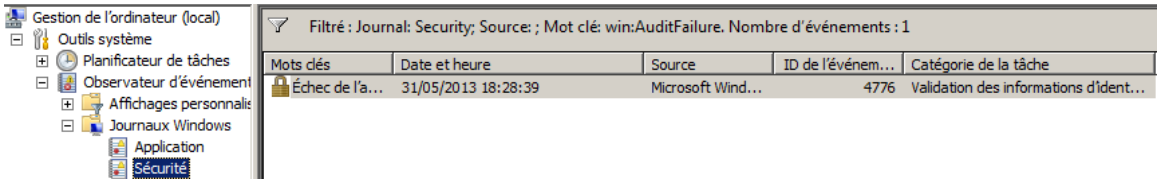
on se plante sur l'ouverture de session, puis on ouvre une session et on retourne voir dans l'observateur d'évènements **Journaux Windows / Sécurité**



on peut **filtrer le journal**



pour obtenir

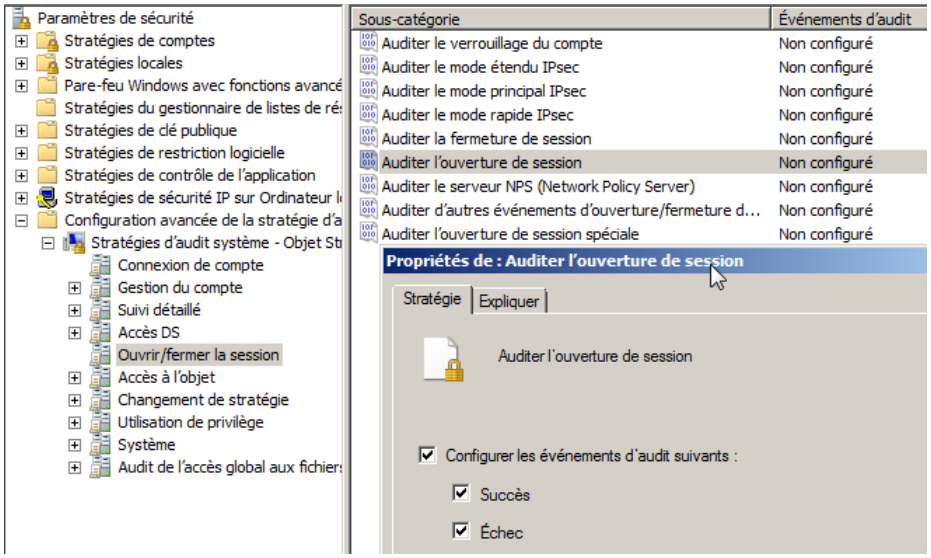


Audit uniquement ouverture de session erronée :

On veut par rapport aux audits armés par défaut sur un poste Windows 10 diminuer le nombre d'événements, et dont après listage des audits, désarmement…

Audits avancé Ouverture fermeture de session

pour armer l'audit sur ouverture de session simple, on peut maintenant que l'on a fait le "ménage " passer par l'interface graphique...



on peut aussi passer par auditpol

auditpol /get /Category:"Ouverture/Fermeture de session"

```
C:\Users\Administrateur>auditpol /get /Category:"Ouverture/Fermeture de session"

Stratégie d'audit système
Catégorie/Sous-catégorie                    Paramètre
Ouverture/Fermeture de session
  Ouvrir la session                         Aucun audit
  Fermer la session                         Aucun audit
  Verrouillage du compte                    Aucun audit
  Mode principal IPsec                      Aucun audit
  Mode rapide IPsec                         Aucun audit
  Mode étendu IPsec                         Aucun audit
  Ouverture de session spéciale             Aucun audit
  Autres événements d'ouverture/fermeture de sessionAucun audit
  Serveur NPS                               Aucun audit
```

On veut armer L'ouverture de session, en Succès et en Echec…

auditpol /get /SubCategory:"Ouvrir la session"

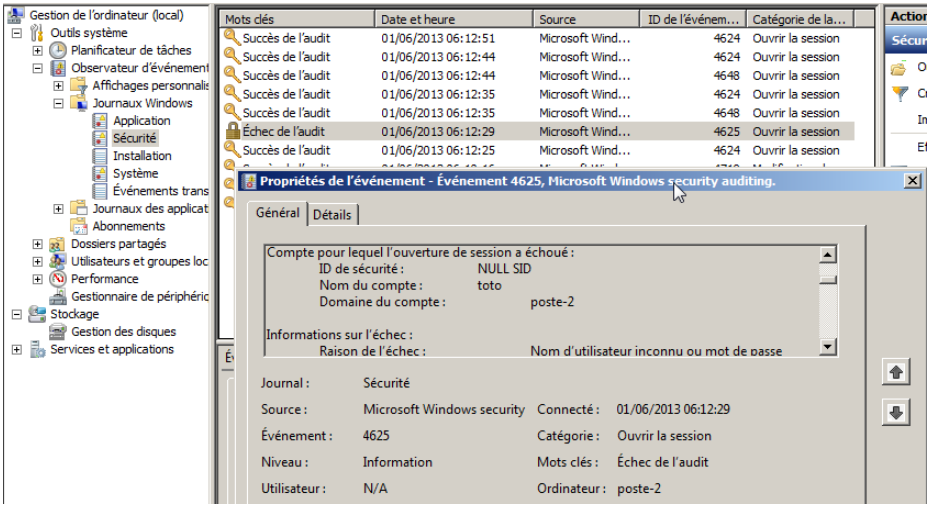
```
C:\Users\Administrateur>auditpol /get /SubCategory:"Ouvrir la session"
Stratégie d'audit système
Catégorie/Sous-catégorie                    Paramètre
Ouverture/Fermeture de session
  Ouvrir la session                         Aucun audit
```

Donc il faut passer

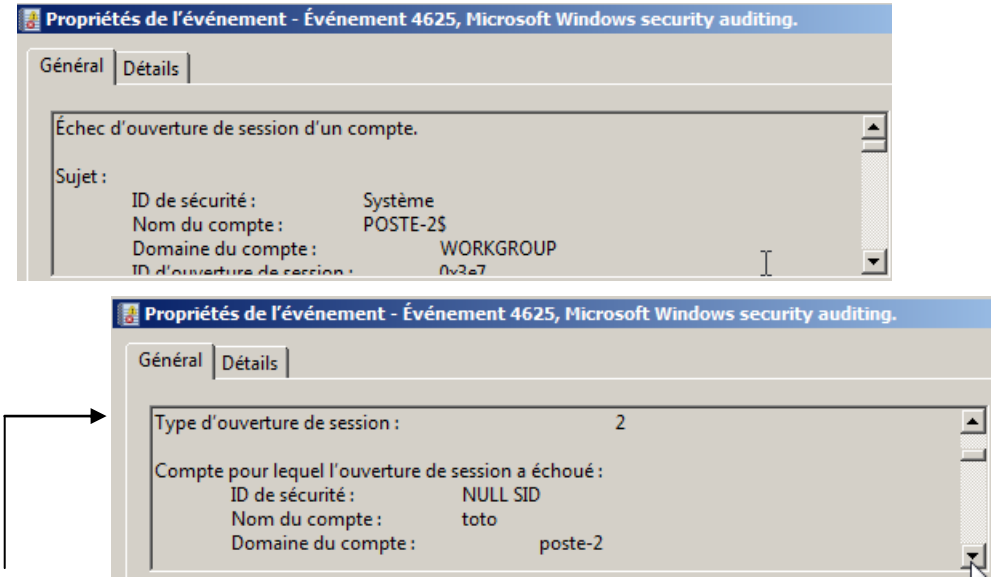
auditpol /set /SubCategory:"Ouvrir la session" /failure:enable /success:enable

```
C:\Users\Administrateur>auditpol /set /SubCategory:"Ouvrir la session" /failure:
enable /success:enable
Commande exécutée correctement.
```

si toto commet une erreur d'ouverture de session , puis Bob et l'administrateur se loguent avec succès, on obtient



dans les informations on a notamment

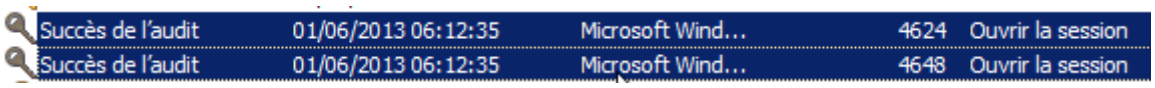


le type **2** signifie une tentative locale,

le type **3** signifie un accès via le réseau...

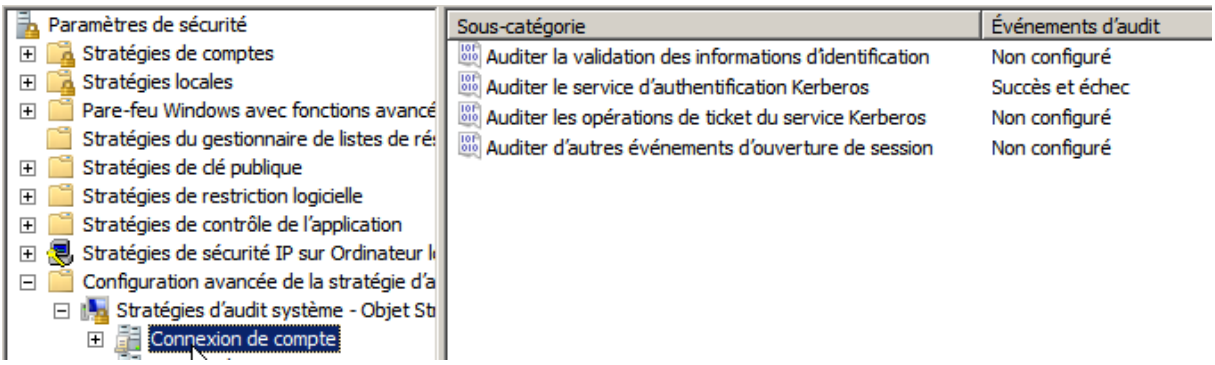
N.B: à chaque échec d'ouverture de session, 1 événement est consigné, pour la tentative d'authentification...

N.B: à chaque ouverture de session, 2 événements sont consignés, un pour la tentative d'authentification, et l'autre pour la réussite d'ouverture de session...

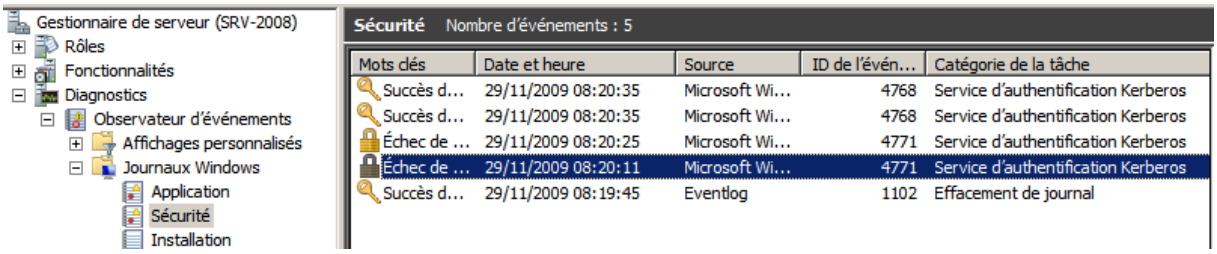


autre méthode, pour avoir le moins d'évènements possible, il faut demander un niveau "avant" la session ouverte ou non", c'est l'authentification…

Auditer le service d'authentification Kerberos



Voici deux tentatives avec mauvais mot de passe, suivies d'une ouverture réussie (qui génère en fait 2 évènements)



Via **auditpol** cela donnerait

```
C:\Users\Administrateur>auditpol /get /Category:"connexion de compte"
Stratégie d'audit système
Catégorie/Sous-catégorie                    Paramètre
Connexion de compte
  Opérations de ticket du service KerberosAucun audit
  Autres événements d'ouverture de sessionAucun audit
  Service d'authentification Kerberos     Succès et échec
  Validation des informations d'identificationAucun audit
```

Il semble donc que la sous catégorie à modifier soit "Service d'authentification Kerberos" mais l'apostrophe régionalisée ne passera pas…

auditpol /set /SubCategory:"Service d'Authentification Kerberos" /failure:enable /success:enable

donnera une erreur…

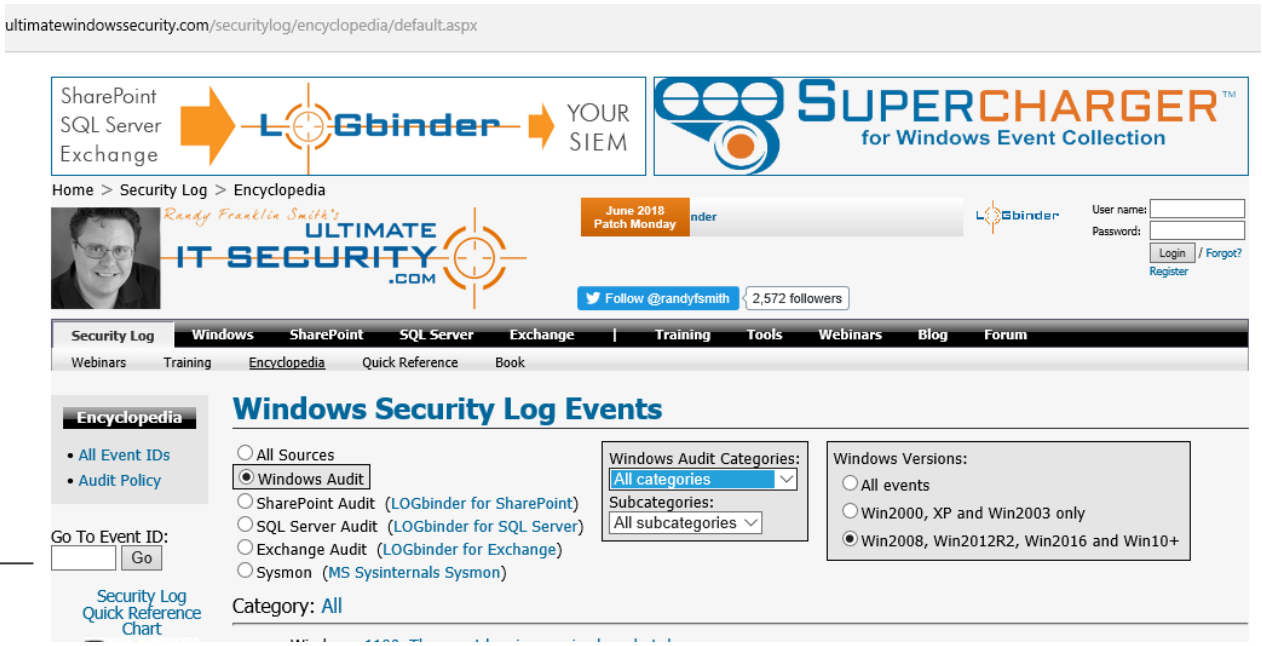
La commande **auditpol /get /Category:"connexion de compte" /r** permet de récupérer le GUID de la sous catégorie

```
C:\Users\Administrateur>auditpol /get /Category:"connexion de compte" /r
Machine Name,Policy Target,Subcategory,Subcategory GUID,Inclusion Setting,Exclus
ion Setting
SRV-2008,System,Opérations de ticket du service Kerberos,{0CCE9240-69AE-11D9-BED
3-505054503030},Aucun audit,
SRV-2008,System,Autres événements d'ouverture de session,{0CCE9241-69AE-11D9-BED
3-505054503030},Aucun audit,
SRV-2008,System,Service d'authentification Kerberos,{0CCE9242-69AE-11D9-BED3-505
054503030},Succès et échec,
SRV-2008,System,Validation des informations d'identification,{0CCE923F-69AE-11D9
-BED3-505054503030},Aucun audit,
```

Et donc on pourra modifier cette sous catégorie par

auditpol /set /SubCategory:"{0CCE9242-69AE-11D9-BED3-505054503030" /failure:enable /success:enable

Il existe des endroits plus informés…



Donnant avec un n° de log

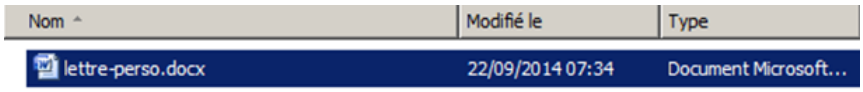
0x6	Client not found in Kerberos database	Bad user name, or new computer/user account has not replicated to DC yet
0x7	Server not found in Kerberos database	New computer account has not replicated yet or computer is pre-w2k
0x8	Multiple principal entries in database	
0x9	The client or server has a null key	administrator should reset the password on the account
0xA	Ticket not eligible for postdating	
0xB	Requested start time is later than end time	
0xC	KDC policy rejects request	Workstation restriction

0x12	Clients credentials have been revoked	Account disabled, expired, locked out, logon hours.
0x13	Credentials for server have been revoked	
0x14	TGT has been revoked	
0x15	Client not yet valid - try again later	
0x16	Server not yet valid - try again later	
0x17	Password has expired	The user's password has expired.
0x18	Pre-authentication information was invalid	Usually means bad password

STRATEGIE AUDIT RESSOURCE DOSSIER

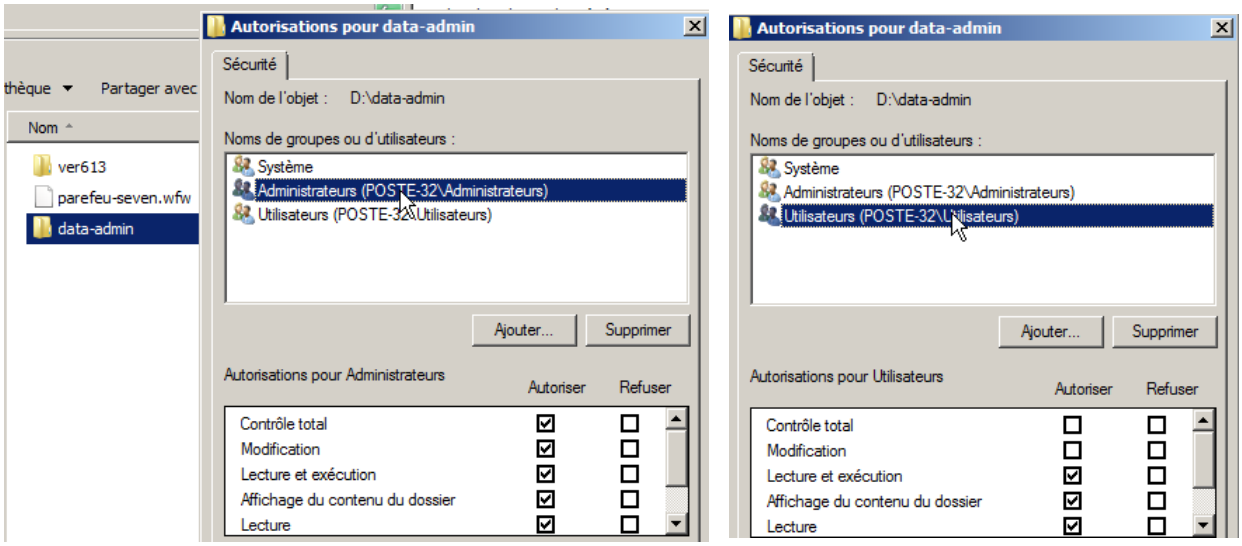
Pister les tentative d'effacement dans un dossier:

On veut savoir qui essaye (alors qu'il n'en a pas le droit) d'effacer des documents



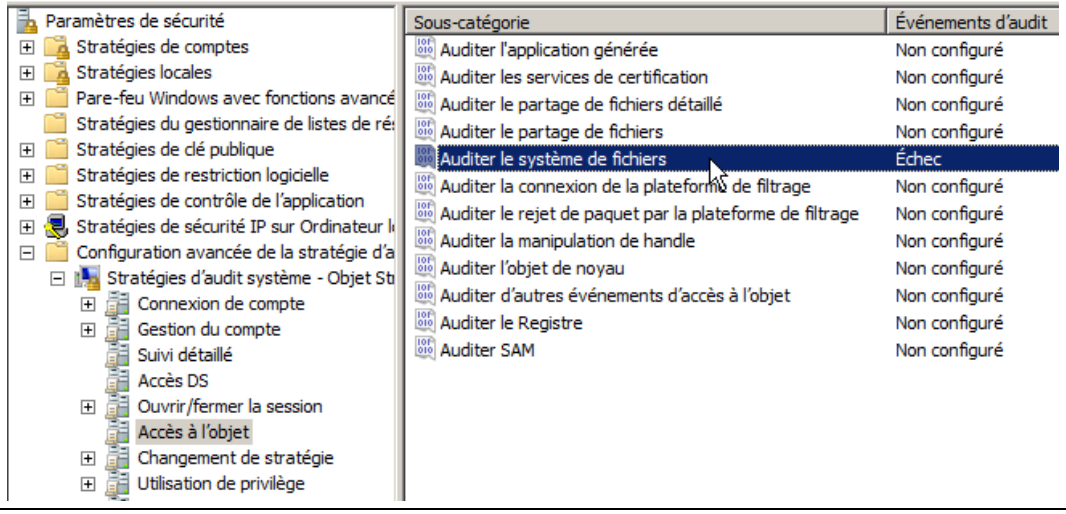
Dans un dossier nommé ***data-admin*** où seuls les **administrateurs** ont tous les droits, et les **utilisateurs** ont un accès en lecture seule

On se crée un dossier Data pour lequel le groupe des **administrateurs** a un accès complet et le groupe des **utilisateurs** ont un accès en lecture seule

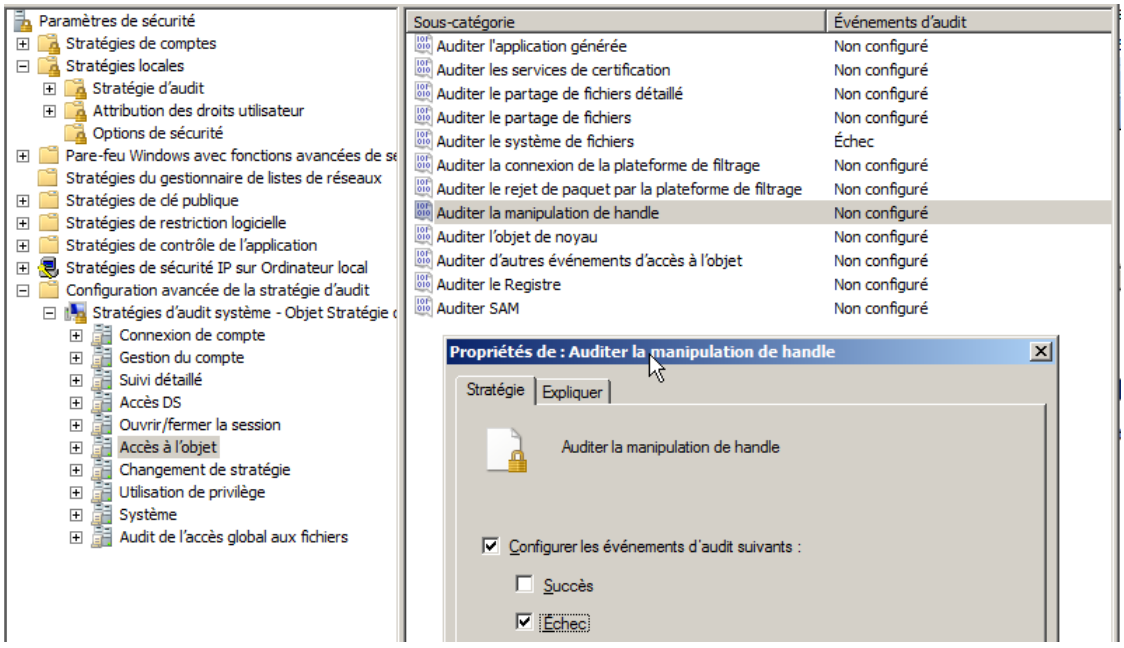


Armement audit Accès l' l'objet + handle:

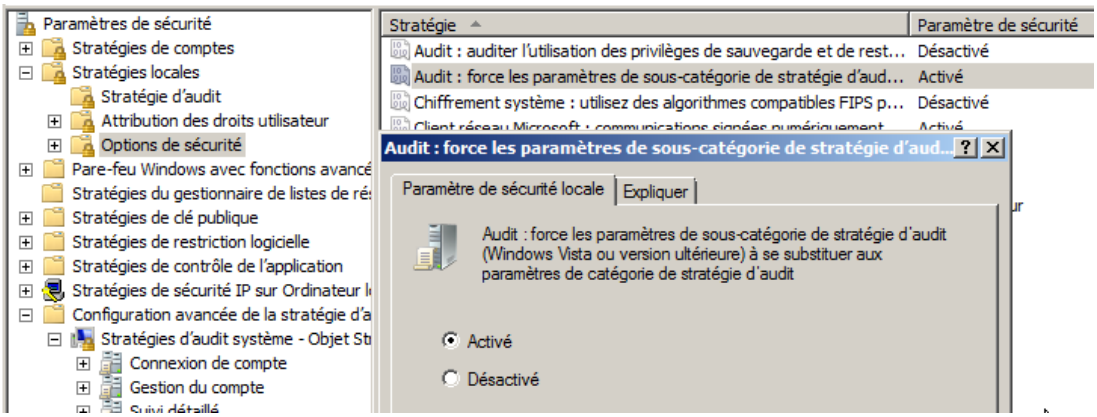
Pour minimiser les évènements on utilise la **configuration avancée de la stratégie d'audit**… On arme en **Echec** le **système de fichier**



et la **manipulation de handle**

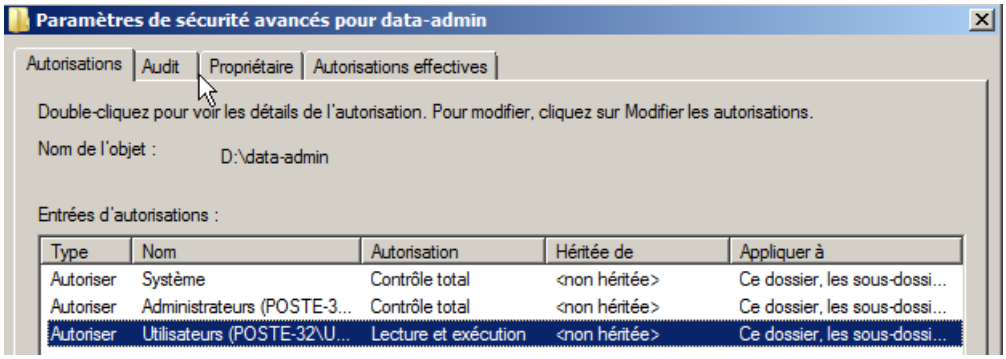


On n'oublie pas d'indiquer que l'on veut utiliser la configuration avancée

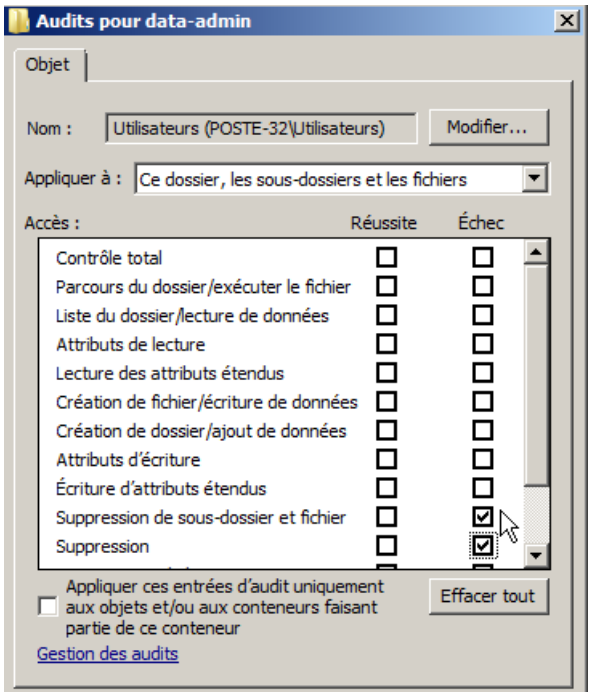


Armement ACL et ACE d'audit

Pour ce dossier ***data-admin*** on va ensuite armer l'audit



On arme l'audite pour le groupe des utilisateurs du poste, en echec de suppression…

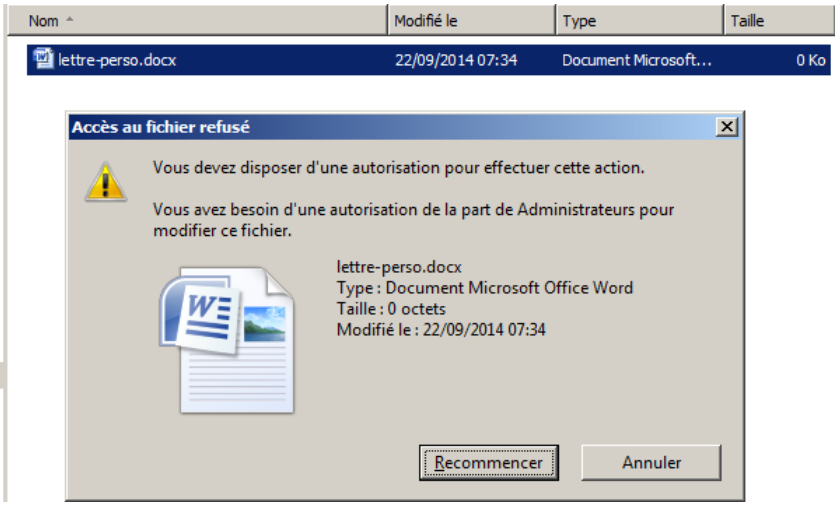


Attention aux nombre d'accès pisté, et pour qui…

Ici on gère uniquement les tentatives d'effacement commises par les utilisateurs locaux du poste…

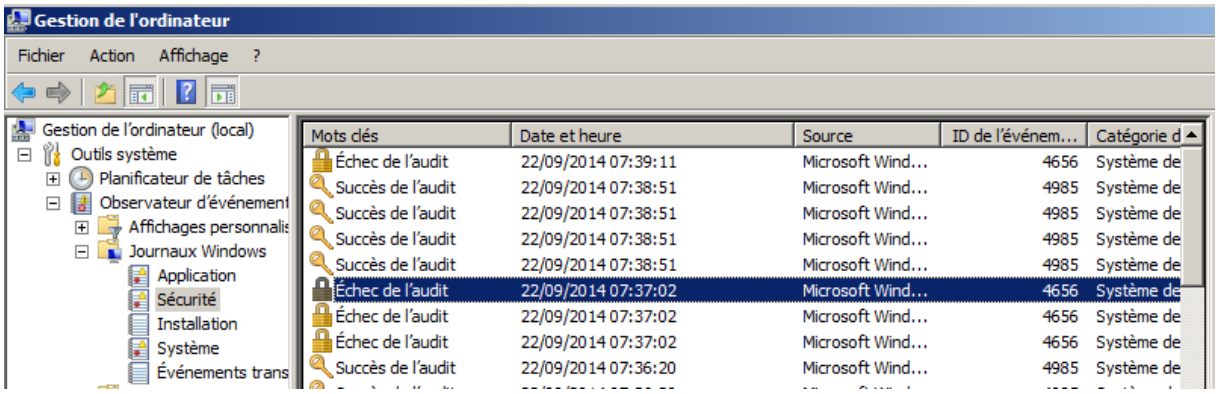
Tentative de suppression (Evenement à auditer)

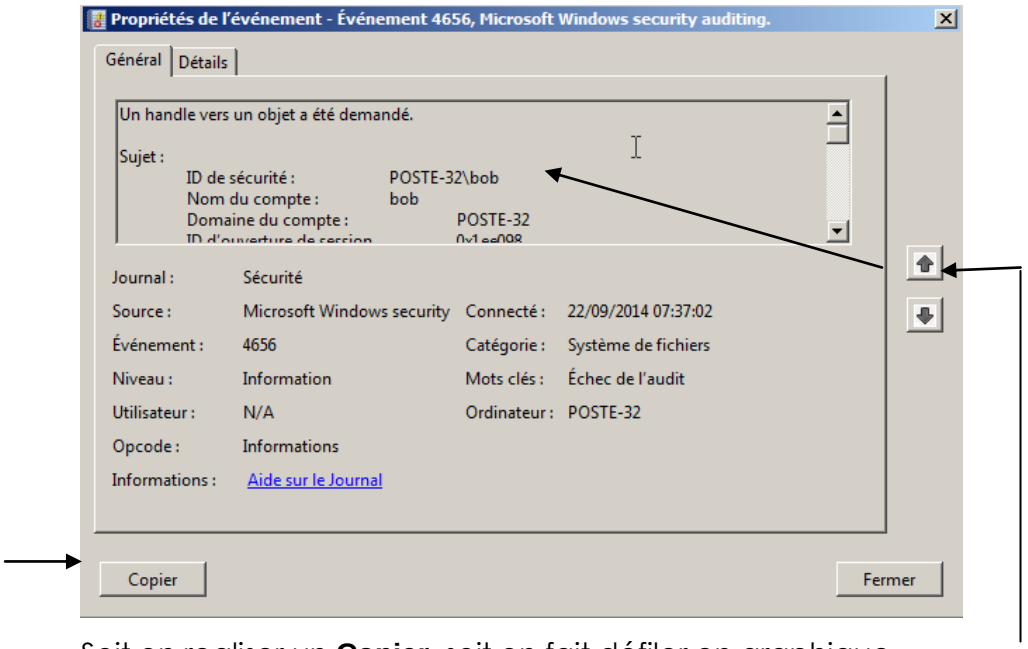
On ouvre une session en tant que ***bob*** et on essaye de supprimer le document…



Lecture du journal

On ouvre la session en ***administrateur*** et on va **dans gestion d'ordinateur**, visualiser le **journal d'évènement / sécurité**





Soit on realiser un **Copier**, soit on fait défiler en graphique…

```
  <Execution ProcessID="504" ThreadID="512" />
  <Channel>Security</Channel>
  <Computer>POSTE-32</Computer>
  <Security />
</System>
<EventData>
  <Data Name="SubjectUserSid">S-1-5-21-3259205789-1686284417-687699897-1005</Data>
  <Data Name="SubjectUserName">bob</Data>
  <Data Name="SubjectDomainName">POSTE-32</Data>
  <Data Name="SubjectLogonId">0x1ee098</Data>
  <Data Name="ObjectServer">Security</Data>
  <Data Name="ObjectType">File</Data>
  <Data Name="ObjectName">D:\data-admin\lettre-perso.docx</Data>
  <Data Name="HandleId">0x0</Data>
  <Data Name="TransactionId">{00000000-0000-0000-0000-000000000000}</Data>
  <Data Name="AccessList">%%1537
                          %%1541
                          %%4423
                          </Data>
  <Data Name="AccessReason">%%1537:      %%1805
                          %%1541:      %%1801      D:(A;ID;0x1200a9;;;BU)
                          %%4423:      %%1811      D:(A;OICI;0x1200a9;;;BU)
                          </Data>
  <Data Name="AccessMask">0x110080</Data>
  <Data Name="PrivilegeList">-</Data>
  <Data Name="RestrictedSidCount">0</Data>
  <Data Name="ProcessId">0x3bc</Data>
  <Data Name="ProcessName">C:\Windows\explorer.exe</Data>
```

STRATEGIE AUDIT RESSOURCE IMPRIMANTE

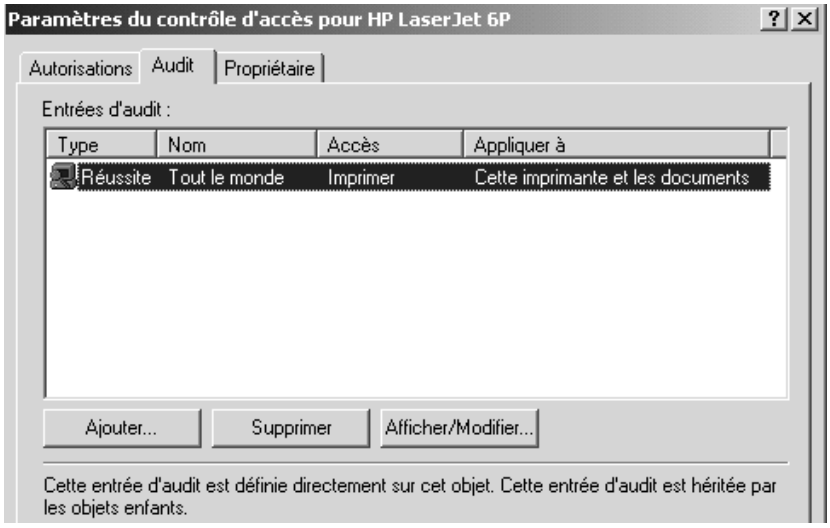
Savoir qui imprime :

Il faut activer l'Audit "**Accès aux objets**" dans les stratégies locales de l'ordinateur sur lequel l'imprimante est connectée.

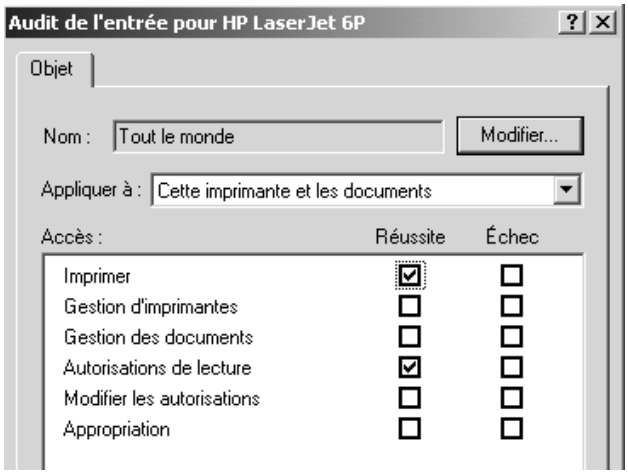
On doit demander **Audit sur Réussite**

Ensuite il faut se placer sur l'imprimante que l'on souhaite auditer, et demander dans les propriétés de l'imprimante:

onglet **Sécurité / Avancées** et onglet **Audit**…



avec



AUDIT EVENEMENT SUR CD

Pister les tentatives d'accès :

Dans une entreprise, on souhaite pister les tentatives d'accès infructueuses effectuées sur le réseau. On souhaite avoir des renseignements lorsque on a des tentatives de connexion qui échouent….

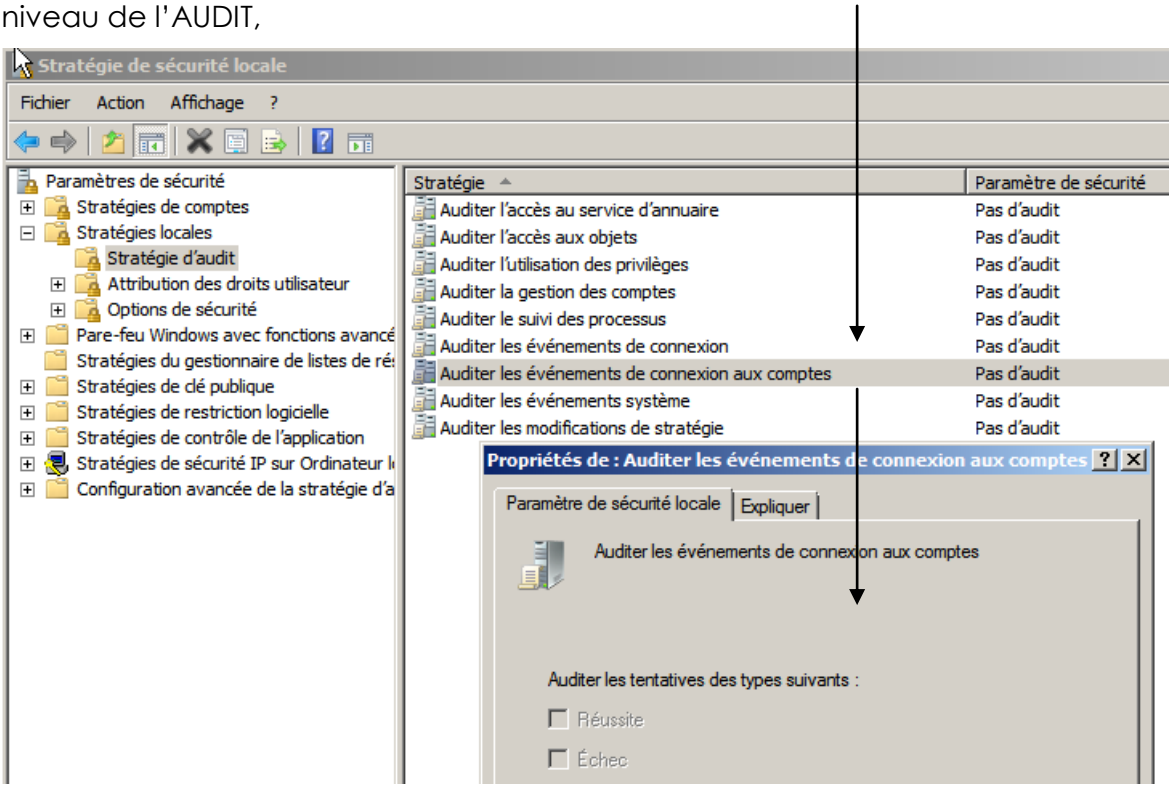
Le principe va consister à armer une stratégie d'audit basée sur les **évènements de connexion aux comptes**.

Par définition on n'auditera que les tentatives qui échouent, en sachant que l'événement est enregistré sur la machine sur laquelle l'identification se fera…

Audit événement de connexion aux comptes sur CD 2008 :

Si on veut une trace des tentatives infructueuses sur le domaine, il faut auditer le contrôleur de domaine…

On voit que les stratégies de sécurité locales ne sont pas disponibles au niveau de l'AUDIT,



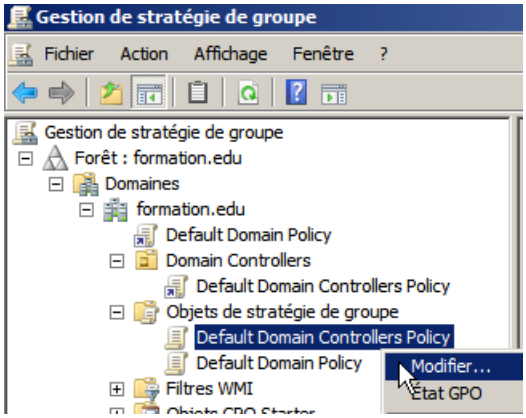
Elles sont remplacées par les stratégies de **Contrôleur de Domaine**…

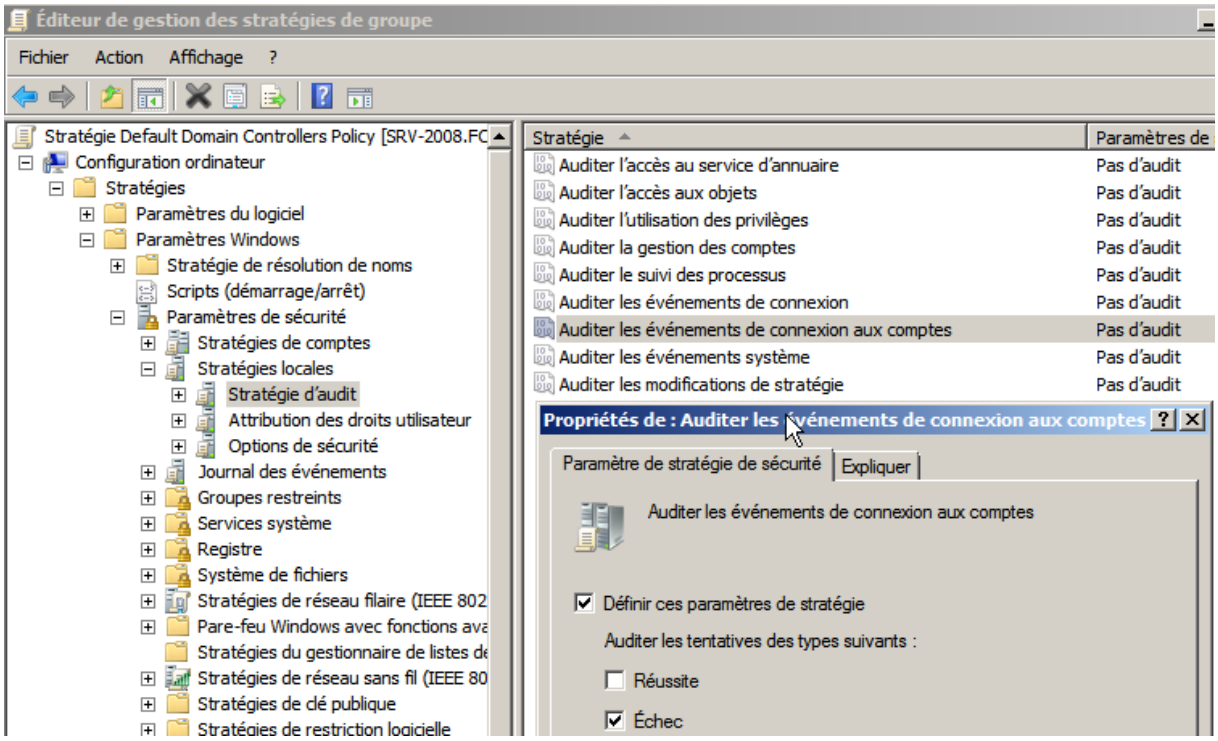
N.B: Uniquement si les stratégies de contrôleur de domaine sont propagées…

On Visualise alors **la Gestion des Stratégies de groupes**

On demande les **Default Domain Controllers policy** = **Stratégies de sécurité des Contrôleurs de Domaine**

NB : Surtout ne pas armer les Default Domain policy = **Stratégies de sécurité du Domaine**





Pour obtenir dans le journal