

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

<u>www.cabare.net</u>©

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	4
AUDIT EVENEMENT – AUDIT RESSOURCE:	4
Installer un Audit sur evenement – 10 - Seven	5
SE PREPARER DANS L'OBSERVATEUR D'EVENEMENT	6
VOIR UN EVENEMENT AUDITE	7
LOCALISATION DES EVENEMENTS	8
LOCALISATION DES JOURNAUX D'EVENEMENT	8
CONFIGURATION DU CLIENT COLLECTE – WINRM – COMPTE ORDI	9
CONFIGURATION DU POSTE COLLECTEUR	
CHOIX DES EVENEMENTS - ABONNEMENT	
CONFIGURATION AVANCEE AUDIT	15
CONFIGURATION AVANCEE DE STRATEGIES D'AUDIT 10 - 7	15
AUDITPOL - LIMITES DE L'INTERFACE GRAPHIQUE	16
AUDITPOL - CATEGORIES ET SOUS CATEGORIES AUDITPOL/LIST:	17
LISTER LES AUDIT AUDITPOL/GET:	17
Modifier les audit auditpol/set:	
DESACTIVER TOUS LES AUDITS	
LIRE LE JOURNAL DE SECURITE:	
INSTALLER UN AUDIT SUR DES RESSOURCES:	
Audit ressource sur un dossier	20
Audit ressource sur une imprimante	
STRATEGIE AUDIT EVENEMENT	25
PISTER LES TENTATIVES D'ACCES :	25
AUDIT EVENEMENT CONNEXION AUX COMPTES SUR UN CLIENT 7 :	
STRATEGIE AUDITPOL	27
AUDIT UNIQUEMENT OUVERTURE DE SESSION ERRONEE :	
AUDITS AVANCE OUVERTURE FERMETURE DE SESSION	
AUDITS AVANCE CONNEXION AUTHENTIFICATION KERBEROS	
INTERPRETATION DES LOG	
STRATEGIE AUDIT RESSOURCE DOSSIER	
PISTER LES TENTATIVE D'EFFACEMENT DANS UN DOSSIER:	
ARMEMENT AUDIT ACCES L' L'OBJET + HANDLE:	
ARMEMENT ACL ET ACE D'AUDIT	
TENTATIVE DE SUPPRESSION (EVENEMENT A AUDITER)	
LECTURE DU JOURNAL	
STRATEGIE AUDIT RESSOURCE IMPRIMANTE	
SAVOIR QUI IMPRIME :	
AUDIT EVENEMENT SUR CD	
PISTER LES TENTATIVES D'ACCES :	
AUDIT EVENEMENT DE CONNEXION AUX COMPTES SUR CD 2008 :	



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

🚡 Stratégie de sécurité locale			
Fichier Action Affichage ? Image: Constraint of the second			
🚡 Paramètres de sécurité	Stratégie	Paramètre de sécurité	
 Stratégies de comptes Stratégies locales Stratégie d'audit Attribution des droits utilisateur Options de sécurité Pare-feu Windows avec fonctions ava Stratégies du gestionnaire de listes de Stratégies de clé publique Stratégies de restriction logicielle Stratégies de sécurité IP sur Ordinateu 	 Auditer la gestion des comptes Auditer l'accès au service d'annuaire Auditer l'accès aux objets Auditer le suivi des processus Auditer les événements de connexion Auditer les événements de connexion aux comptes Auditer les événements système Auditer les modifications de stratégie Auditer l'utilisation des privilèges 	Pas d'audit Pas d'audit Pas d'audit Pas d'audit Pas d'audit Pas d'audit Pas d'audit Pas d'audit Pas d'audit	1

par exemple sur évènements de connexion aux comptes

	Propriétés	de : Auditer les év	vénements d	e connexion aux c	?	×	
	Paramètre	de sécurité locale	Expliquer				
et en demandant d'auditer les Réussites et/ou les Echec		Auditer les événer	nents de conn	exion aux comptes			
	Audi	ter les tentatives de: Réussite	s types suivan	ts :			
	→ 🥂	chec					
par exemple on souhaite ici pister les tentatives d'accès avec un mot de passe erroné pour obtenir donc après une	1	Il est possible que c stratégie est configu au niveau de la cat Pour obtenir davant événements de cor	ce paramètre n urée pour avoi régorie. tage d'informal nnexion aux co	e soit pas appliqué si ur r la priorité sur la stratég tions, consultez <u>Auditer</u> o <u>mptes</u> . (Q921468)	ne autre ie d'audit <u>les</u>		
tentative d'ouverture erroné	ée						

🚡 Paramètres de sécurité	Stratégie	Paramètre de sécurité
> 📴 Stratégies de comptes	📓 Auditer l'accès au service d'annuaire	Pas d'audit
 Stratégies locales 	Auditer l'accès aux objets	Pas d'audit
> 📴 Stratégie d'audit	Auditer l'utilisation des privilèges	Pas d'audit
Attribution des droits utilisateur	Auditer la gestion des comptes	Pas d'audit
> G Options de sécurité	Auditer le suivi des processus	Pas d'audit
Pare-feu Windows avec fonctions ava Charténies du participanies de lister de	Auditer les événements de connexion	Pas d'audit
Strategies du gestionnaire de listes de Stratégies de clé publique	Auditer les événements de connexion aux comptes	Échec



Stratégies et GPO Audit windows 10 AD 2012R2 - 2016 - SYS 26- Cours - ver 2.6 - http://www.cabare.net Page 5 - Michel Cabaré -

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

🞥 Gestion de l'ordinateur				
Fichier Action Affichage ?				
🗢 🔿 📶 🔢 🖬				
Gestion de l'ordinateur (local)	Mots clés	Date et heure	Source	ID
Outlis systeme Dianificateur de tâcher	🔒 Échec de l'audit	15/12/2015 11:56:59	Microsof	
V Planincaleur de lacries V Planincaleur d'événements	🔒 Échec de l'audit	09/07/2018 07:10:29	Microsof	
Affichages personnalisés	🔒 Échec de l'audit	09/07/2018 06:36:29	Microsof	
V 📑 Journaux Windows	🔍 Succès de l'audit	05/07/2018 06:10:12	Microsof	
Application	🔍 Succès de l'audit	05/07/2018 06:10:14	Microsof	
📔 Sécurité	🔍 Succès de l'audit	05/07/2018 06:10:12	Microsof	
Installation	Succès de l'audit	05/07/2018 06:10:19	Microsof	

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

🛃 Gestion de l'ordinateur		\mathbb{N}
Fichier Action Affichage ?	Propriétés des vues persor	nnalisées X
 Gestion de l'ordinateur (local) Outils système Outils système Observateur d'événements Observateur d'événements Affichages personnalisés Événements d'admini cechec audit Journaux Windows Application Sécurité Installation Système Événements transférés Monnements Monnements Monnements Obssiers partagés Willisateurs et groupes locaux Sectorade Gestionnaire de périphérique Stockage Services et applications 	Filtrer XML Connecté : Niveau d'événement : Niveau d'événement : Niveau d'événement : Par journal Par source Inclut/exclut des ID d'ét séparant par des virgule Par exemple 1,3,5-99,-7 Catégorie de la tâche : Mots clés : Utilisateur : Ordinateur(s) :	À tout moment Critique Avertissement Critique Avertissement Critique Avertissement Critique Avertissement Critique Avertissement Critique Avertissement Durnaux d'événements: Image: Commentaires Journaux d'événements: Image: Commentaires Sources d'événements: Image: Commentaires vénements: entrez les numéros ou les plages d'identificateurs en les es. Pour exclure des critères, faites-les précéder du signe amoins ». 6 Tous les ID d'événements> Image: Commentaires Échec de l'audit Image: Commentaires Image: Commentaires <



Stratégies et GPO Audit windows 10 AD 2012R2 - 2016 - SYS 26- Cours - ver 2.6 - http://www.cabare.net Page 6 - Michel Cabaré -

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**

 Gestion de l'ordinateur (local) ¹Outils système Outils système Ole Planificateur de tâches <u>II</u> Observateur d'événeme Observateur d'événeme Observateur d'événeme 	Nom Nom Administrat DefaultAcco Invité	Nom complet
 Willisateurs et groupes I 	🌺 util	util
Utilisateurs		

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

Propriétés de	l'événement - Événement 477	^{76,} Microsoft V	Vindows security auditing.	×
Général Détai L'ordinateur a Package d'au Compte d'ou	ls a tenté de valider les information thentification : MICRO verture de session : util	ons d'identifica SOFT_AUTHEI	ation d'un compte. NTICATION_PACKAGE_V1_0	
Station de tra Code d'erreu	vail source : PORT-P16 🔓			
Source :	Securite Microsoft Windows security	Connecté	00/07/2018 08-30-17	
Événement :	4776	Catégorie :	Validation des informations d'identification	•
Niveau :	Information	Mots-clés :	Échec de l'audit	
Utilisateur :	N/A	Ordinateur :	PORT-P16.cabare-intra.net	



Stratégies et GPO Audit windows 10 AD 2012R2 - 2016 - SYS 26- Cours - ver 2.6 - http://www.cabare.net Page 7 - Michel Cabaré -

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**

軇 Gestion de l'ordinateur	
Fichier Action Affichage ?	
🗢 🄿 📊 🗟 🖬	
🔙 Gestion de l'ordinateur (local)	Nom
> 👔 Outils système	Se connecter à un autre ordinateur

puis renseigner les champs de la boîte de dialogue

Sélectionner un ordinateur	?	×
Sélectionnez l'ordinateur devant être géré par ce composant logiciel enfichable.		
Ce composant logiciel enfichable gérera toujours :		
C L'ordinateur local (l'ordinateur sur lequel cette console s'exécute)		
Un autre ordinateur : \\port-p16	Parcourir	
\triangleright		

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 dis TYPE STATE WIN32_EXIT_CODE SERVICE_EXIT_CODE	tance de Windows (Gestion WSM) : 20 WIN32_SHARE_PROCESS : 1 STOPPED : 1077 (0x435) : 0 (0x0)	
🔍 Services		
Gestion à distance de Windows (Gestion WSM) <u>Démarrer</u> le service	Nom Des Gestion à distance de Windows (Gestion WSM) Le s Gestion d'applications Tra Gestion d'application à distance de Windows (Gestion à	cription service Gestion à distance ite les demandes d'installa tion WSM) (Ordi X
Description : Le service Gestion à distance de Windows implémente le protocole Gestion des services Web pour la gestion à distance. La Gestion des services Web est un protocole standard utilisé pour la gestion à distance de logiciels et de matériels. Le service Gestion à distance de Windows traite les demandes Gestion des services Web. Il doit être configuré à l'aide de l'outil winrm.cmd ou via la stratégie de groupe. Ce service donne accès aux données WMI et permet le recueil d'événements. Le recueil d'événements et l'abonnement	Griefinal Connexion Récupération Dépendances Griefinal Connexion Récupération Dépendances Griefinal Nom du service : WinRM Griefinal Nom complet : Gestion à distance de Windows Griefinal Description : Le service Gestion à distance de mplémente le protocole Gestion Griefinal Chemin d'accès des fichiers exécutables : C:\Windows\System32\svchost.exe +k NetworkServ Griefinal Griefinal Manuel Griefinal H État du service : Artifié	(Gestion WSM) Windows des services Web
distance de Windows utilisent HTTP et HTTPS. Le service Gestion à	H Démarrer Arrêter Suspendre	Reprendre

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 quickconfi WinRM n'est pas configuré pour recev Les modifications suivantes doivent	g oir des demandes sur cet ordinateur. être effectuées :
Démarrez le service WinRM. Affectez un démarrage automatique à	retardement au service WinRM.
Effectuer ces modifications [y/n] ?	у

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 ${\bf y}$ et on enchaine



Cela peut aussi se faire en Powershell par la commande

Enable-psremoting

PS C:\Windows\system32> <mark>Enable-psremoting</mark> 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

Gestion de l'ordinateur (local)	Nom Administrateurs	Description Les membres du groupe Administ		
 > I Observateur d'événements > I Dossiers partagés 	Propriétés de : Admin	istrateurs	?	×
 Willisateurs et groupes locaux Utilisateurs Groupes M Performance Gestionnaire de périphériques Stockage 	Description :	టు eurs Les membres du groupe Administrateurs dispose complet et illimité à l'ordinateur et au domaine	nt d'un accè	ès
 Gestion des disques Services et applications 	Membres : Administrateur CABARE-INTRA CABARE-INTRA	\\Admins du domaine \\PORT-P9		



Stratégies et GPO Audit windows 10 AD 2012R2 - 2016 - SYS 26- Cours - ver 2.6 - http://www.cabare.net Page 10 - Michel Cabaré - Il faut ajouter le service réseau dans le groupe des Lecteurs des journaux d'évènement de la machine auditée/collectée.

 Willisateurs et groupes l Utilisateurs Groupes 	Martins_IUSKS	es journaux d'événe	ements	Groupe integre utilise par les Les membres du groupe Invit Des membres de ce groupe p	servi és di euve	
N Performance Gestionnaire de périphé	Pr	ropriétés de : Lecteu	urs des journau	ux d'événements	?	×
Stockage Gestion des disques	A Opérat	Général	6			
Services et applications	A System	Lecteurs o	des journaux d'é	vénements		
	A Utilisat	Description :	Des membres d événements à j	le ce groupe peuvent lire les journ partir de l'ordinateur local	aux des	
	A Utilisat Utilisat	Membres :	SERVICE RÉS	SEAU (S-1-5-20)		

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

v 🖥	Paramètres de sécurité	La penoguer les programmes	Automistrateurs
5	Stratégies de comptes	Effectuer les tâches de maintenance de volume	Administrateurs
ý	A Stratégies locales	Emprunter l'identité d'un client après l'authentification	SERVICE LOCAL, SERVICE RÉSEA
	> 🔀 Stratégie d'audit	Forcer l'arrêt à partir d'un système distant	Administrateurs
	> 🛃 Attribution des droits utili:	Générer des audits de sécurité	SERVICE LOCAL, SERVICE RÉSEAU
	> 🔀 Options de sécurité	Gérer le journal d'audit et de sécurité	SERVICE RÉSEAU, Administrateurs
	-		

Configuration du poste Collecteur

Il faut activer le service Windows Event collector.

Un sc query type= service state= all donnerait





Stratégies et GPO Audit windows 10 AD 2012R2 - 2016 - SYS 26- Cours - ver 2.6 - http://www.cabare.net Page 11 - Michel Cabaré - 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

Propriétés de l'abonnement	- audit session poste p16	2		×	(
Nom d'abonnement :	audit session poste p16				
Description :				0	
	L				
Journal de destination :	Événements transférés			~	
Type d'abonnement et ord	linateurs sources				
Initialisation par le col	lecteur		Sélectionner de	es ordinateurs 🔺	
Cet ordinateur conta	cte les ordinateurs sources sélec	ctionnés et	fournit l'abonne	ement.	
O Initialisation par l'ordi	nateur source	Sélection	ner des groupes	d'ordinateurs	
Les ordinateurs source la configuration locale	s dans les groupes sélectionnés pour contacter cet ordinateur e	doivent êt et recevoir	re configurés av l'abonnement.	ec la stratégie ou	
Événements à recueillir :	<filtre configuré="" non=""></filtre>	:	Sélectionner des	événements	
Compte d'utilisateur (le cor	mpte sélectionné doit avoir acc	ès en lectu	re aux journaux s	ources) :	
Compte d'ordinateur					
Modifier un compte d'utilis	ateur ou configurer les paramè	tres avancé	és :	Avancé	
			OK	Annuler	



Stratégies et GPO Audit windows 10 AD 2012R2 - 2016 - SYS 26- Cours - ver 2.6 - http://www.cabare.net Page 12 - Michel Cabaré -

Sélectionner des ordinateurs Ordinateurs (1): Nom port-p16.cabare-intra.net Observateur d'événements Tester Observateur d'événements CK OK Ajouter des ordi. du domaine... Supprimer Tester

et faire un filtre de requête

Filtre de requête		×
Filtrer XML		
Connecté :	À tout moment ~	
Niveau d'événement :	Critique Avertissement Commentaires	
	Erreur Information	
Par journal	Journaux d'événements : Sécurité	Ī
O Par source	Sources d'événements : Journaux Windows	
Inclut/exclut des ID d'é séparant par des virgule Par exemple 1,3,5-99,-7	vénements : entrez les numér es. Pour exclure des critères, f 6 < Tous les ID d'événements Justallation Système Événements transférés Journaux des applications et des	
Catégorie de la tâche :		Í

Et doit obtenir

£ 1
Evenements transferes

On peut via clic droit

Nom	Statut	Туре	Ordinateur Journal de dest Description
🕖 audit poste 16	Actif	Initialisatio	1 Événements tra
			Supprimer
			État d'exécution
			Propriétés 😼
			Désactiver
			Réessayer



Stratégies et GPO Audit windows 10 AD 2012R2 - 2016 - SYS 26- Cours - ver 2.6 - http://www.cabare.net Page 13 - Michel Cabaré -



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

🔙 Gestion de l'ordinateur (local)	Niveau	Date et heure	Source II	D de l'	Catégo	Journal	01 ^
Outils système	(i) Information	09/07/2018 12:28:28	Micros	4672	Special	Sécurité	PC
> Planificateur de tâches		00/07/2010 12:20:20	Micros	4624	Logon	Cácuritá	DC
Observateur d'événements		09/07/2010 12:20:20	MICIOS	4024	Logon	Securite	PC
> 購 Affichages personnalisés	Information	09/07/2018 12:11:23	Micros	4672	Special	Securite	PC
🗸 📑 Journaux Windows	(i) Information	09/07/2018 12:11:23	Micros	4624	Logon	Sécurité	PC
Application	(i) Information	09/07/2018 12:10:54	Micros	4634	Logoff	Sécurité	PC
Sécurité	 Information 	09/07/2018 12:09:29	Micros	4634	Logoff	Sécurité	PC
Installation	(i) Information	09/07/2018 12:09:29	Micros	4634	Logoff	Sécurité	PC
💽 Système	Information	09/07/2018 12:09:07	Micros	4634	Logoff	Sécurité	РС
Événements transférés	1 Information	09/07/2018 12:08:59	Micros	4624	Logon	Sécurité	PC
🗸 💾 Journaux des applications et de	(i) Information	09/07/2018 12:08:59	Micros	4672	Special	Sécurité	PC
😭 Internet Explorer	(i) Information	09/07/2018 12:08:59	Micros	4672	Special	Sécurité	PC
> 📔 Microsoft	(i) Information	09/07/2018 12:08:57	Micros	4634	Logoff	Sécurité	PC
😭 Microsoft Office Alerts	(i) Information	09/07/2018 12:08:57	Micros	4624	Logon	Sécurité	PC
Service de gestion de clés	(i) Information	09/07/2018 12:08:57	Micros	4672	Special	Sécurité	PC
Windows PowerShell	 Information 	09/07/2018 12:08:57	Micros	4672	Special	Sécurité	PC
Evénements matériels	(i) Information	09/07/2018 12:08:57	Micros	4634	Logoff	Sécurité	PC 🗸
Abonnements	<						>
> bossiers partagés	f. (Mining A Mining and A					~
> 🗿 Utilisateurs et groupes locaux	Evenement 4072,	ivilcrosoft windows security a	auditing.				
> (N) Performance	Général Détail	s					
Gestionnaire de peripheriques							^
> E Stockage	Source :	Microsoft Windows security	Connecté :	09/07/2	2018 12:28:2	28	
> is services et applications	Événement :	4672	Catégorie :	Special	l Logon		
	Niveau :	Information	Mots-clés :	Succès	de l'audit		
	Utilicateur	N/A	Ordinateur	PORT-	D16 cabare	intra net	
	ounsateur :	N/A	orumateur :	FORT	FIOCODATE	muanet	



Stratégies et GPO Audit windows 10 AD 2012R2 - 2016 - SYS 26- Cours - ver 2.6 - http://www.cabare.net Page 14 - Michel Cabaré -

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

🚡 Paramètres de sécurité	Stratégie 🔺	Paramètre 🔺
🗄 📴 Stratégies de comptes	🖾 Audit : arrêter immédiatement le système s'il n'est pas possible de	Désactivé
🖃 📴 Stratégies locales	💹 Audit : auditer l'accès des objets système globaux	Désactivé
🙀 Stratégie d'audit	Audit : auditer l'utilisation des privilèges de sauvegarde et de rest	Désactivé
王 📴 Attribution des droits utilisateur	Audit : force les paramètres de sous-catégorie de stratégie d'aud	Non défini
🙀 Options de sécurité	Chiffrement système : utilisez des algorithmes compatibles EIPS p	Désactivé
Pare-feu Windows avec fonctions avancées de sécurité		·
Stratégies du gestionnaire de listes de réseaux	Audit : force les paramètres de sous-catégorie de stratégie d'	aud <mark>?</mark> 🗙
🕀 🧰 Stratégies de clé publique		
El Stratégies de restriction logicielle	Parametre de secunte locale Expliquer	
El Stratégies de contrôle de l'application	Audit : force los paramètros de sous esté este de statégie d'	
표 🛃 Stratégies de sécurité IP sur Ordinateur local	Windows Vista ou version ultérieure) à se substituer aux	
Configuration avancée de la stratégie d'audit	paramètres de catégorie de stratégie d'audit	
🖃 🌆 Stratégięs d'audit système - Objet Stratégie de groupe local		
표 📑 Confrèxion de compte		
표 📑 Gestion du compte	C Activé	
표 📑 Suivi détaillé	C Discript	
🕀 📑 Accès DS	Desactive	



Stratégies et GPO Audit windows 10 AD 2012R2 - 2016 – SYS 26- Cours - ver 2.6 - http://www.cabare.net Page 15 - Michel Cabaré -

AuditPol - limites de l'interface graphique

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

effaçons le journal

Gestion de l'ordinateur (local)	Mots dés	Date et heure	Source
🖃 🎁 Outils système	Succès de l'audit	31/05/2013 19:08:25	Eventioa
🕀 🕒 Planificateur de tâches			
Observateur d'événement			
🗄 📑 Affichages personnalis			
🖃 📫 Journaux Windows			
Application			
😭 Sécurité			
Installat Ouvrir	le journal enregistré		
Système Créer u	une vue personnalisée		
Événem Import	er une vue personnalisée		
🕀 📑 Journaux de	1		
Abonnemen Efface	r le journal.		
Filtrer	e journal actນiel		

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

🚡 Paramètres de sécurité 🛨 📴 Stratégies de comptes 🗄 📑 Stratégies locales 🔋 Stratégies du gestionnaire de listes de réseaux 🕀 📔 Stratégies de clé publique El Stratégies de restriction logicielle

- El Stratégies de contrôle de l'application
- 표 🛃 Stratégies de sécurité IP sur Ordinateur local
- 🖃 📋 Configuration avancée de la stratégie d'audit
- 🖃 🔚 Stratégies d'audit système Objet Stratégie de groupe local
 - Connexion de compte
 Gestion du compte
 Suivi détaillé

 - Accès DS Ouvrir/fermer la session Accès à l'objet Changement de stratégie

 - 🕀 📑 Audit de l'accès global aux fichiers

Configuration avancée de la stratégie d'audit

Mise en route

Les paramètres de la configuration avancée de la stratégie d'audit peuvent être utili assurer un contrôle détaillé sur les stratégies d'audit, identifier les attaques tentées o votre réseau et vos ressources, et vérifier le respect des règles régissant la gestion c organisationnelles critiques.



Lorsque des paramètres de la configuration avancée de la stratégie d'audit le paramètre de stratégie « Audit : force les paramètres de sous-catégorie d d'audit (Windows Vista ou version ultérieure) à se substituer aux paramètres

En savoir plus sur la configuration avancée de l'audit

Quelles éditions de Windows prennent en charge la configuration avancée de l'

Un résumé des paramètres est présenté ci-dessous :					
Catégories	Configuration				
Connexion de compte	Non configuré				
Gestion du compte	Non configuré				
Suivi détaillé	Non configuré				
Accès DS	Non configuré				
Ouvrir/fermer la session	Non configuré				
Accès à l'objet	Non configuré				
Changement de stratégie	Non configuré				
Utilisation de privilège	Non configuré	N			
Système	Non configuré	3			
Audit de l'accès global aux fichiers	Non configuré				

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



Stratégies et GPO Audit windows 10 AD 2012R2 - 2016 - SYS 26- Cours - ver 2.6 -

http://www.cabare.net Page 16 - Michel Cabaré -

Auditpol - Catégories et Sous catégories auditpol/list:

On peut lister les 10 catégories auditpol/list /category



Lister les audit auditpol/get:

lister tous les audits auditpol/get /category :*

C:\Users\Administrateur>auditpol/get /cat	egory:*
strategie d'audit systeme Catégonie/Sous-catégonie	Panamètne
Sacegorie/Sous cacegorie Sustème	1 41-4112 61-6
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 /Ca	ategory:"système"
Strategie d'audit système Catégorie/Sous-catégorie	Paramètre
Système Extension système de sécurité	Aucun audit
Intégrité du système Pilote IPSEC	Succès et échec Aucun audit
Autres événements système Modification de l'état de la sécurité	Succès et échec Opération réussie

Par défaut

Et visualiser une par une

auditpol /get /SubCategory:"intégrité du système"

C:\Users\Administrateur>auditpol /ge	et /SubCategory:"intégrité du système"
Catégorie/Sous-catégorie	Paramètre
système Intégrité du système	Succès et échec



Stratégies et GPO Audit windows 10 AD 2012R2 - 2016 - SYS 26- Cours - ver 2.6 -

http://www.cabare.net Page 17 - Michel Cabaré -

Et les modifier, globalement par catégories complète

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



donc au final désactivant tous les audits système...

Désactiver tous les audits

il faut pour chaque catégorie la lister via

auditpol /get /category:"xxxxxx"

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



Stratégies et GPO Audit windows 10 AD 2012R2 - 2016 – SYS 26- Cours - ver 2.6 - http://www.cabare.net Page 18 - Michel Cabaré -

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	
Sustème de fichiens	Aucup audit
Registre	Aucun audit
Objet de nouau	Aucun audit
SAM	Aucun audit
Services de certification	Aucun audit
Généré nar annlication	Aucun audit
Manipulation de bandle	Aucun audit
Partage de fichiers	Aucun audit
Rejet de paquet par la plateforme de fi	ltrageAucun 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 priv	ilègesAucun audit
	A
FIN AU PROCESSUS	Aucun audit
HCC1V1CE DFHFI	Aucun audit
Evenements KPG	Aucun audit
Greation au processus	Hucun audit
Changement de stratégie	
Modification de la stratégie d'audit	Aucun audit
Modification de la stratégie d'authenti	ficationAucun audit
Modification de la stratégie d'autorisa	tionAucun audit
Modification de la stratégie de niveau	règle MPSSVCAucun audit
Modification de la stratégie de platefo	rme de filtrageAucun audit
Autres événements de modification de st	ratégieAucun audit
	-
Gestion des comptes	A
Gestion des comptes d'utilisateur	Hucun audit
Gestion des comptes d'ordinateur	Hucun audit
Gestion des groupes de securite	Hucun audit
Gestion des groupes de distribution	Hucun audit
Gestion des groupes d'applications	Hucun audit
Hutres evenements de gestion des comptes	SHUCUN AUGIT
Accès DS	
Modification du service d'annuaire	Aucun audit
Bénlication du service d'annuaire	Aucun audit
Réplication du service d'annuaire détai	lléAucun audit
Accès au service d'annuaire	Aucun audit
Connexion de compte	A
Operations de ticket du service Kerbero	sHucun audit
I HUTWES EUENEMENTS d'AUUENTUNE de sessio	A 114
	nAucun audit
Service d'authentification Kerberos	nAucun audit Aucun audit
Service d'authentification Kerberos Validation des informations d'identific	nAucun audit Aucun audit ationAucun audit

Et que l'on efface ensuite le journal...

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

🛃 Gestion de l'ordinateur					
Fichier Action Affichage ?					
🗢 🔿 🔰 🖬 🚺					
Gestion de l'ordinateur (local)	Mots dés	Date et heure	Source	ID de l'événem	Catégorie de la tâche
🖃 🎁 Outils système	Q Succès de l'a	01/06/2013 05:57:51	Eventlog	1100	Service en cours d'arrêt
() Planificateur de täches () Servateur d'événement	Q Succès de l'a	01/06/2013 05:57:37	Eventlog	1102	Effacement de journal
Affichages personnalis					
Journaux windows Application					
Sécurité					



Stratégies et GPO Audit windows 10 AD 2012R2 - 2016 - SYS 26- Cours - ver 2.6 - http://www.cabare.net Page 19 - Michel Cabaré -

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...

E Gestion de l'ordinateur					
Fichier Action Affichage	?				
🗢 🄿 🔁 🖬 🚺					
Gestion de l'ordinateur (loca	l) Mots clés	Date et heure		Source	ID de l'événe
Outils systeme	Succès de l'audit	27/11/2009 17:3	37:26	Microsoft Wi	4719
A Deservateur d'événer	Succès de l'audit	27/11/2009 17:3	37:26	Microsoft Wi	4719
Affichages person	Succès de l'audit	27/11/2009 17:3	37:26	Microsoft Wi	4719
Journaux Window	/s Succès de l'audit	27/11/2009 17:3	4:59	Microsoft Wi	4634
🗐 Application	🔍 Succès de l'audit	27/11/2009 17:3	3:37	Microsoft Wi	4672
Sécurité	🔍 Succès de l'audit	27/11/2009 17:3	3:37	Microsoft Wi	4624
Setup	Ouvrir le journal enregistré		3-27	Microsoft Wi	4648
🛃 Système	Créer une vue personnalisé	ée			
Evénem	Importer une vue personna	alisée	curity auditing.		
Dournaux de	importer and rac personni				
Abonneme	Effacer le journal				
Bill Dossiers partag	Filtrer le journal actuel	•			
p and ourisateurs et g					

Dans lequel on peut indiquer par exemple dans notre cas

Filtrer XML	
Connecté :	À tout moment
Niveau d'événement i	Critique Avertissement Commentaires
d evenement :	Erreur Information
Par journal	Journaux d'événements : Sécurité
Par source	Sources d'événements :
Inclut/exclut des ID séparant par des vir Par exemple 1,3,5-9	i d'événements : entrez les numéros ou les plages d'identificateurs en rgules. Pour exclure des critères, faites-les précéder du signe « moins 9,-76
Inclut/exclut des ID séparant par des vir Par exemple 1,3,5-9	d'événements : entrez les numéros ou les plages d'identificateurs en rgules. Pour exclure des critères, faites-les précéder du signe « moins 19,-76 <tous d'événements="" id="" les=""></tous>
Inclut/exclut des ID séparant par des vin Par exemple 1,3,5-9 Catégorie de la tâche :	u d'événements : entrez les numéros ou les plages d'identificateurs en rgules. Pour exclure des critères, faites-les précéder du signe « moins 19,-76 <tous d'événements="" id="" les=""></tous>

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...ll 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

II 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...

proprietes de dossier de pierre			
Général Partage Sécurité Versions précédentes	Personna	aliser	
Nom de l'objet : F:\dossier de pierre			
Groupes ou noms d'utilisateurs :			
Legistre (PC-DE-UTIL\pierre)			
& Admir Arateurs (PC-de-util Administrateurs)			
Pour modifier les autorisations, cliquez sur Modifier.		Modifier	
			_
Autorisations pour pierre	Autoriser	Refuser	
Contrôle total			*
Modification	~		
Lecture et exécution	~		=
Affichage du contenu du dossier	~		

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...

	Paramètres	de sécurité av	ancés pour d	lossier de	pierre						x
A	utorisations	Audit Proprie	étaire Autorisa	ations effe	ctives						
	Pour afficher Nom de l'obje Entrées d'au	rou modifierles ∢ et : F:∖dossier dit :	létails d'une er de pierre	trée d'aud	lit, sélecti	onnez l	'entrée, pui	is cliquez su	r Modifier.		
	Туре	Nom		Accès			Héritée d	e	Appliquer à		
 :0	faut e rrespor	ensuite c ndant à	ijouter	pour	qui	et	<u>quel</u>	type	d'Audit	l'on	veut



	Audit de l'entrée po	our dossier de pierre			
	Dbjet				
	Nom : Utilisateurs	authentifiés	Modifier		
	Appliquer Ce dos	sier, les sous-dossiers et les	fichiers 🔻		
	Accès :	Réussite	Échec		
	Contrôle total Parcours du dossier Liste du dossier/lec Attributs de lecture Lecture des attribu Création de fichier/ Création de dossier Attributs d'écriture Écriture d'attributs Suppression de sou Suppression Appliquer ces entre aux objets et/ou a partie de ce conter Gestion des audits	<pre>/exécuter le fichier ture de données ts étendus écriture de donn /ajout de données étendus s-dossier et fichier étes d'audit uniquement ux conteneurs faisant heur</pre>	Effacer tout	Les types d'a tentative de su peuvent être ob Suppression N.B : Ne pas co les accès c génère d'évènements d	audit en ppression tenus par cher tous ar cela autant e plus !!!
Lorsque ensuite un	Mots clés	Date et heure	Source	ID de l'événe Catégorie de l 🍐	
utilisateur tiers	Échec de l'audit	27/11/2009 18:11:39	Microsoft Wi	4656 Système de fi	
essaye d'effacer	🔒 Échec de l'audit	27/11/2009 18:11:39	Microsoft Wi	4656 Système de fi	
le dossier cela	🔍 Succès de l'audit	27/11/2009 18:11:01	Microsoft Wi	4672 Ouverture de	
sora tracó	Succès de l'audit	27/11/2009 18:11:01	Microsoft Wi	4624 Ouvrir la sessi	
seru nuce	Succes de l'audit	27/11/2009 18:11:01	Microsoft Wi	4624 Ouvrir la sessi	
	Succès de l'audit	27/11/2009 18:11:01	Microsoft Wi	4040 Ouvin la sessi	
	•		III	4	
	Événement 4656, Mie	crosoft Windows security aud	liting.	×	
	Général Détails				
	Un handle vers u Sujet : ID de sé Nom du Domain ID d'ouv Objet : Serveur	n objet a été demandé. curité : PC-de-ut i compte : util e du compte : rerture de session : de l'objet : Sécurité	iil\util PC-de-util 0x20189e Security		
	Source :	Microsoft Windows secu	rity Connecté :	27/11/2009 18:11:39	

Audit ressource sur une imprimante

On veut savoir qui utilise l'imprimante réellement :

Événement :

4656

ll faut

1. activer l'Audit "Accès aux objets" en succès dans les stratégies locales de l'ordinateur sur lequel l'imprimante est connectée...

Catégorie :

2. sur cette imprimante demander par les Propriétés avancées NTFS onglet Sécurité, puis bouton Avancé



Système de fichiers

General	Partage	Ports	Avancé
Gestion des coule	urs Sécurité	Paramètre	s du périphérique
roupes ou noms d'u	tilisateurs :		
👫 Tout le monde		2	
🗟 CREATEUR PR	OPRIETAIRE	20	
🔏 Administrateur (F	PC-de-util\Administrateu	ır)	
👫 Administrateurs ((PC-de-util\Administrate	urs)	
		Ajouter	Supprimer
utorisations pour To	ut le monde	Autoris	ser Refuser
Imprimer		V	
Gestion d'impriman	tes		
Gestion des docun	nents		
Autorisations spéci	iales		

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

📔 Paramètre	s de sécurité avan	cés pour HP LaserJet 6P			×
Autorisations	Audit Propriétai	re Autorisations effective	3		
Pour affiche	r ou modifier les déta	ails d'une entrée d'audit, sé	lectionnez l'entrée, puis clique:	z sur Modifier.	
Entrées d'au	ıdit :	la l			
Туре	Nom	Accès	Héritée de	Appliquer à	

Et il faut indiquer ce que l'on veut auditer

Audit de l'entrée pour HP LaserJet 6P					
Objet					
Nom : Utilisateurs authentifiés		Modifier			
Appliquer Cet objet et les obj	ets enfants	Ŧ			
Accès :	Réussite	Échec			
Imprimer	5				
Gestion d'imprimantes	-3				
Gestion des documents					
Autorisations de lecture	V				
Modifier les autorisations					
Appropriation					

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)	🤿 Filtré :Journal	: Security; Source: M	icrosoft-Windows-	-Security-Auditin	g; Catégorie de la f	tâche: Autres
a 🎁 Outils système						
Planificateur de tâches	Mots clés	Date et heure		Source	ID de l'événe	Catégorie de 📤
Ø Observateur d'événeme	Succès de l'aud	it 27/11/2009 18:29	:07	Microsoft Wi	4656	Autres évén
Affichages personna	🔍 Succès de l'aud	it 27/11/2009 18:29	:07	Microsoft Wi	4658	Autres évén
Journaux Windows	🔍 Succès de l'aud	it 27/11/2009 18:26	:17	Microsoft Wi	4656	Autres évén
Application	🔍 Succès de l'aud	it 27/11/2009 18:26	:17	Microsoft Wi	4658	Autres évén
Securite	🔍 Succès de l'aud	it 27/11/2009 18:26	:17	Microsoft Wi	4656	Autres évén 🔻
Setup	•					•
👔 Systeme	Événement 4656, N	licrosoft Windows s	ecurity auditing.			×
Journaux des applica	Général Détails	1				
📑 Abonnements	betans					
Dossiers partagés	TD de	- 6î k 6 -	DC de util\Adusi			
Willisateurs et groupes I	Nom	du compte :	Administrateur	nistrateur		
Fiabilité et performance	Doma	ine du compte :	PC-de-u	ıtil		
🛃 Gestionnaire de périphé	ID d'o	uverture de session :	0x23d6c	8		E
▲ 🔄 Stockage						
Gestion des disques	Objet :	1.0.1.1.		l	de la companya de la	
Services et applications	Serve	ur de l'objet : d'objet :	Spooler			
	Nom	de l'obiet :	HP LaserJet 6P			
	ID du	handle	0v1765078			Ŧ



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 <u>sur la machine sur laquelle l'identification se fera</u>...

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



Stratégies et GPO Audit windows 10 AD 2012R2 - 2016 – SYS 26- Cours - ver 2.6 - http://www.cabare.net Page 25 - Michel Cabaré -

🚂 Gestion de l'ordinateur					
Fichier Action Affichage ?					
🗢 🔿 📩 🖬 🛛 🖬					
Eestion de l'ordinateur (local)	Mots dés	Date et heure	Source	ID de l'évé	Catégorie de la tâche
🖃 🎁 Outils système	🔍 Succès	31/05/2013 18:21:39	Microsoft Windows security au	4719	Modification de la stratégie d'audit
Planificateur de tâches	Succès	31/05/2013 18:21:39	Microsoft Windows security au	4719	Modification de la stratégie d'audit
Boservateur d'événements	🔍 Succès	31/05/2013 18:21:39	Microsoft Windows security au	4719	Modification de la stratégie d'audit
Affichages personnalises	🔍 Succès	31/05/2013 18:21:39	Microsoft Windows security au	4719	Modification de la stratégie d'audit
	Succès	31/05/2013 18:20:23	Microsoft Windows security au	4648	Ouvrir la session
	🔍 Succès	31/05/2013 18:20:18	Microsoft Windows security au	4648	Ouvrir la session
Sécurité	🔍 Succès	31/05/2013 18:19:54	Microsoft Windows security au	4634	Fermer la session
Installation	🔍 Succès	31/05/2013 18:19:53	Microsoft Windows security au	4672	Ouverture de session spéciale
Système	Événement 4	648, Microsoft Windows se	curity auditing.		
Événements transférés	· · ·				
Durnaux des applications et des services	Général [)étails			
internet Explorer					
Key Management Service	Tentative	d'ouverture de session en	utilisant des informations d'identificat	tion explicites.	
Media Center					
Microsoft Microsoft Microsoft	Sujet :	10 1 2 3 2			
Événements matériels		ID de securite : Nom du compto :	Administrateur	т	
Abonnements		Domaine du compte :	poste-2	T	

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**

😓 Gestion de l'ordinateur (local)	Mots dés	Date et heure	Source	ID de l'événem	Catégorie de la tâche
Outils système	🔍 Succès de l'a	31/05/2013 18:29:15	Microsoft Wind	4648	Ouvrir la session
Planificateur de täches	🔍 Succès de l'a	31/05/2013 18:28:58	Microsoft Wind	4634	Fermer la session
Boservateur d'evenement	🔍 Succès de l'a	31/05/2013 18:28:45	Microsoft Wind	4672	Ouverture de session spéciale
Affichages personnalis	🔍 Succès de l'a	31/05/2013 18:28:45	Microsoft Wind	4624	Ouvrir la session
	🔍 Succès de l'a	31/05/2013 18:28:45	Microsoft Wind	4648	Ouvrir la session
	🔍 Succès de l'a	31/05/2013 18:28:45	Microsoft Wind	4776	Validation des informations d'ident
Jostallation	Échec de l'a	31/05/2013 18:28:39	Microsoft Wind	4776	Validation des informations d'ident
	Q Succès de l'a	31/05/2013 18:28:30	Microsoft Wind	4647	Fermer la session
Événements trans	Succès de l'a	31/05/2013 18:21:39	Microsoft Wind	4719	Modification de la stratégie d'audit
🕀 🦰 Journaux des applicat	Événement 4776	Microsoft Windows security auditir	in a		
Abonnements	Evenement 4770,	Where some windows security addition	'9'		
🛨 🔞 Dossiers partagés	Général Détai	s			
🛨 🌆 Utilisateurs et groupes loc		•			
	L'ordinateur a	tenté de valider les informations d	identification d'un	compte	
📇 Gestionnaire de périphériq		tente de valuer les informations d	identification d'un	compter	
🖃 🔄 Stockage	Package d'au	thentification : MICROSOFT	AUTHENTICATIO	N_PACKAGE_V1_0	
Gestion des disques	Compte d'ou	verture de session : admin 🕌			
 Envices et applications 	Station de tra	vail source : POSTE-2			
	Code d'erreur	: 0xc000006a			

on peut filtrer le journal

🚂 Gestion de l'ordinateur		
Fichier Action Affichage ?	Filtrer le journal actuel)
🗢 🔿 🖄 🖬 🛛 🗖	Filtrer XML	
Gestion de l'ordinateur (local)	Connecté : À tout moment	.
 Planificateur de tâches Observateur d'événement 	Niveau d'événement : 🗖 Critique 🗖 Avertissement 🗖 Commentaires	
 Affichages personnalis Journaux Windows 	Erreur Information	
Application	Par journal Journaux d'événements: Sécurité] [
Installation	O Par source Sources d'événements :] [
 Evénements trans Journaux des applicat Abonnements 	Inclut/exclut des ID d'événements : entrez les numéros ou les plages d'identificateurs en les séparant par des virgules. Pour exclure des critères, faites-les précéder du signe « moins ». Par exemple 1 3 5-99 -76	
	Tous les ID d'événements>	
① Performance Gestionnaire de périphéric	Catégorie de la tâche :	
Stockage Gestion des disques	Mots clés : Échec de l'audit	
🛨 📷 Services et applications		

pour obtenir





Stratégies et GPO Audit windows 10 AD 2012R2 - 2016 - SYS 26- Cours - ver 2.6 - http://www.cabare.net Page 26 - Michel Cabaré -

STRATEGIE AUDITPOL

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 /C	ategory:"Ouverture/Fermeture de session"
Stratégie d'audit système Catégorie/Sous-catégorie	Pavamètre
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	e 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.



Stratégies et GPO Audit windows 10 AD 2012R2 - 2016 - SYS 26- Cours - ver 2.6 - http://www.cabare.net Page 27 - Michel Cabaré - si toto commet une erreur d'ouverture de session , puis Bob et l'administrateur se loguent avec succès, on obtient

Carting de Kastraders (Last)			1	1		
Gestion de l'ordinateur (local)	Mots clés	Date et heure	Source	ID de l'événem	Catégorie de la	Action
E Cutils systeme	🔍 Succès de l'audit	01/06/2013 06:12:51	Microsoft Wind	4624	Ouvrir la session	Sécur
Planificateur de taches	🔍 Succès de l'audit	01/06/2013 06:12:44	Microsoft Wind	4624	Ouvrir la session	
Observateur d'evenement	🔍 Succès de l'audit	01/06/2013 06:12:44	Microsoft Wind	4648	Ouvrir la session	_ [@] [∪]
Affichages personnalis	🔍 Succès de l'audit	01/06/2013 06:12:35	Microsoft Wind	4624	Ouvrir la session	- III 💎 o
- Journaux windows	🔍 Succès de l'audit	01/06/2013 06:12:35	Microsoft Wind	4648	Ouvrir la session	
Application	🔒 Échec de l'audit	01/06/2013 06:12:29	Microsoft Wind	4625	Ouvrir la session	
Securite Installation	Succès de l'audit	01/06/2013 06:12:25	Microsoft Wind	4624	Ouvrir la session	E
	Q <u>~</u>	01/05/0040.05 40.45	the Article	1710	A 10 11 1	
E Événomente trans	🧧 🛃 Propriétés de l'év	vénement - Événement 46	25, Microsoft Wind	dows security aud	iting.	×
Conservent de la popicat Conservent ados Abornements Aborneme	Général Détails Compte pour leq ID de sé Nom du Domain Informations sur Raison d Journal : Source : É Vénement : Viveau : Utilisateur :	juel l'ouverture de session a d curité NULL SIE a compte : toto le du compte : l'échec : de l'échec : Sécurité Microsoft Windows security 4625 Information N/A	śchoué :) poste-2 Nom d'utilisateur Connecté : 01/ Catégorie : Ou Mots clés : Éch Ordinateur : pos	inconnu ou mot de 06/2013 06:12:29 vrir la session nec de l'audit :te-2	e Dasse	+

dans les informations on a notamment

Échec d'o	uverture de session d'un c	ompte.			_
Sujet : II D T	D de sécurité : Jom du compte : Jomaine du compte : D d'ouverture de cersion :	Système POSTE-2\$ WORK 0v3=7	GROUP	I	T
8	Propriétés de l'événeme	ent - Événemer	nt 4625, Microsoft W	indows security	auditing.
	Général Détails				
→	Type d'ouverture de ses	sion :	2		
	Compte pour lequel l'ou ID de sécurité :	uverture de sessi NU	on a échoué : LL SID		
	Nom du comp	te: toto			

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...

-						
_	- I IV IV.	and the state of t		and Channel I		
	Echoc do l'audit		2 05 13 30	Microsoft Wind	4675	Ouwrin la coccion
	ieu ieu ue rauuri	01/00/20	J UU: 12:23			OUVER RESSIULT

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...

	M				
٩	Succès de l'audit	01/06/2013 06:12:35	Microsoft Wind	4624	Ouvrir la session
٩	Succès de l'audit	01/06/2013 06:12:35	Microsoft Wind	4648	Ouvrir la session



Audits avancé Connexion authentification kerberos

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

haramètres de sécurité	Sous-catégorie	Événements d'audit
표 📴 Stratégies de comptes	🕮 Auditer la validation des informations d'identification	Non configuré
🕀 📴 Stratégies locales	Auditer le service d'authentification Kerberos	Succès et échec
🕀 🚞 Pare-feu Windows avec fonctions avancé	Auditer les opérations de ticket du service Kerberos	Non configuré
Stratégies du gestionnaire de listes de ré:	Auditer d'autres événements d'ouverture de session	Non configuré
표 📔 Stratégies de clé publique		
🛨 🧮 Stratégies de contrôle de l'application		
🗉 🛃 Stratégies de sécurité IP sur Ordinateur k		
🖃 📋 Configuration avancée de la stratégie d'a		
🖃 🌆 Stratégies d'audit système - Objet Sti		
🗉 🚰 Connexion de compte		

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

Gestionnaire de serveur (SRV-2008)	Sécurité Non	nbre d'événements : 5			
Roles Fonctionnalités	Mots dés	Date et heure	Source	ID de l'évén	Catégorie de la tâche
 Diagnostics 	Succès d	29/11/2009 08:20:35	Microsoft Wi	4768	Service d'authentification Kerberos
Observateur d'événements	Succès d	29/11/2009 08:20:35	Microsoft Wi	4768	Service d'authentification Kerberos
표 📑 Affichages personnalisés	Échec de	29/11/2009 08:20:25	Microsoft Wi	4771	Service d'authentification Kerberos
🖃 📫 Journaux Windows	Échec de	29/11/2009 08:20:11	Microsoft Wi	4771	Service d'authentification Kerberos
Application	Succès d	29/11/2009 08:19:45	Eventlog	1102	Effacement de journal
😭 Sécurité					
Installation					

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 Ker Autres égénements d'ougerture de se	berosAucun audit ssionAucun audit
Service d'authentification Kerberos	Succès et échec
Validation des informations d'ident	ificationAucun 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,<OCCE9240-69AE-11D9-BED 3-505054503030},Aucun audit, SRV-2008,System,Autres événements d'ouverture de session,<OCCE9241-69AE-11D9-BED 3-505054503030},Aucun audit, SRV-2008,System,Service d'authentification Kerberos,<OCCE9242-69AE-11D9-BED3-505 054503030},Succès et échec, SRV-2008,System,Validation des informations d'identification,<OCCE923F-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



Interpretation des Log

Il existe des endroits plus informés...





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	h.
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

Nom ^	Modifié le	Туре
📓 lettre-perso.docx	22/09/2014 07:34	Document Microsoft

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

	🕌 Autorisations pour data-admin		×	🔒 Autorisations pour data-adm	in	×
	Sécurité			Sécurité		
thèque 🔻 Partager avec	Nom de l'objet : D:\data-admin			Nom de l'objet : D:\data-admin		
Nom *	Noms de groupes ou d'utilisateurs :			Noms de groupes ou d'utilisateurs :		
🎳 ver613	& Système			& Système		
parefeu-seven.wfw	Administrateurs (POSTE-32\Adm	inistrateurs)		Administrateurs (POSTE-32\Ad	ministrateurs)	
🕌 data-admin	Utilisateurs (POSTE-32&Utilisateu)	ırs)		Utilisateurs (POSTE-32\L\tisate	eurs)	
		Ajouter	Supprimer		Ajouter	Supprimer
	Autorisations pour Administrateurs	Autoriser	Refuser	Autorisations pour Utilisateurs	Autoriser	Refuser
	Contrôle total	\checkmark		Contrôle total		
	Modification			Modification		
	Lecture et exécution			Lecture et exécution		
	Affichage du contenu du dossier			Affichage du contenu du dossier		
	Lecture			Lecture		

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



Stratégies et GPO Audit windows 10 AD 2012R2 - 2016 – SYS 26- Cours - ver 2.6 - http://www.cabare.net Page 32 - Michel Cabaré -

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

🖥 Paramètre	es de sécurité avancés po	ur data-admin		×
Autorisations	Audit Propriétaire Autoris	sations effectives		
Double-cliqu	iez pour voir les détails de l'aut	orisation. Pour modifier, o	cliquez sur Modifier les au	itorisations.
Nom de l'obj	jet : D:\data-admin			
Entrées d'au	toriostiona -			
Entrees d'au	uonsauons .			
Туре	Nom	Autorisation	Héritée de	Appliquer à
Autoriser	Système	Contrôle total	<non héritée=""></non>	Ce dossier, les sous-dossi
Autoriser	Administrateurs (POSTE-3	Contrôle total	<non héritée=""></non>	Ce dossier, les sous-dossi
Autoriser	Utilisateurs (POSTE-32\U	Lecture et exécution	<non héritée=""></non>	Ce dossier, les sous-dossi

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



퉬 Audits pour data-admin	×
Objet	
Nom : Utilisateurs (POSTE-32\Utilisateurs)	Modifier
Appliquer a : Ce dossier, les sous-dossiers et les f	ichiers 📩
Accès : Réussite	Échec
Contrôle total Parcours du dossier/exécuter le fichier Liste du dossier/lecture de données Attributs de lecture Lecture des attributs étendus Création de fichier/écriture de données Attributs d'écriture Écriture d'attributs étendus Suppression de sous-dossier et fichier Suppression Appliquer ces entrées d'audit uniquement	
aux objets et/ou aux conteneurs faisant partie de ce conteneur <u>Gestion des audits</u>	

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...

Nom *		Modifié le	Туре	Taille
🔨 lettre-perso	.docx	22/09/2014 07:34	Document Microsoft	0 Ко
Accès au	I fichier refusé Vous devez disposer d'une au Vous avez besoin d'une autor modifier ce fichier. Iettro Type Taille Mod	torisation pour effectuer sation de la part de Adm perso.docx :: Document Microsoft (:: 0 octets fié le : 22/09/2014 07:34	cette action. iinistrateurs pour Office Word	X
		Recommencer	Annuler	1

Lecture du journal

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

🛃 Gestion de l'ordinateur					
Fichier Action Affichage ?					
🗢 🔿 🖄 🖬 🛛 🖬					
Gestion de l'ordinateur (local)	Mots dés	Date et heure	Source	ID de l'événem	Catégorie d 🔺
🖃 🎁 Outils système	🔒 Échec de l'audit	22/09/2014 07:39:11	Microsoft Wind	4656	Système de
Planificateur de täches	🔍 Succès de l'audit	22/09/2014 07:38:51	Microsoft Wind	4985	Système de
Observateur d'evenement	🔍 Succès de l'audit	22/09/2014 07:38:51	Microsoft Wind	4985	Système de
+ Affichages personnalis	🔍 Succès de l'audit	22/09/2014 07:38:51	Microsoft Wind	4985	Système de
	🔍 Succès de l'audit	22/09/2014 07:38:51	Microsoft Wind	4985	Système de
	Échec de l'audit	22/09/2014 07:37:02	Microsoft Wind	4656	Système de
	🔒 Échec de l'audit	22/09/2014 07:37:02	Microsoft Wind	4656	Système de
Système	🔒 Échec de l'audit	22/09/2014 07:37:02	Microsoft Wind	4656	Système de
Événements trans	Succès de l'audit	22/09/2014 07:36:20	Microsoft Wind	4985	Système de
	• • • • • • • • • • • • • • • • • • •				



Stratégies et GPO Audit windows 10 AD 2012R2 - 2016 - SYS 26- Cours - ver 2.6 - http://www.cabare.net Page 34 - Michel Cabaré -

Sujet :	ID de sécurité : Nom du compte : Domaine du compte : ID d'ouverture de session	POSTE-32\bob bob POSTE-32 0v1 ee008	I	
Journal :	Sécurité			
Source :	Microsoft Window	ws security Connecté :	22/09/2014 07:37:02	
Événemer	nt: 4656	Catégorie :	Système de fichiers	
Niveau :	Information	Mots clés :	Échec de l'audit	
Utilisateur	: N/A	Ordinateur :	POSTE-32	
Opcode:	Informations			
Informatio	ons : <u>Aide sur le Journa</u>	al		

Soit on realiser un Copier, soit on fait défiler en graphique...

<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="SubjectUserName">bob</Data> <Data Name="SubjectUserName">bob</Data> <Data Name="SubjectUserName">bob</Data> <Data Name="SubjectLogonId">0x1ee098</Data> <Data Name="SubjectLogonId">0x1ee098</Data> <Data Name="ObjectServer">Security</Data> <Data Name="ObjectType">File</Data> <Data Name="ObjectType">File</Data> <Data Name="ObjectType">File</Data> <Data Name="ObjectName">D:\data-admin\lettre-perso.docx</Data> <Data Name="Handleld">0x0</Data> <Data Name="TransactionId">{00000000-0000-0000-0000-00000000000}</Bata>

<Execution ProcessID="504" ThreadID="512" />

<Data Name="AccessList">%%1537

%%1541 %%4423

</Data>

<Data Name="AccessReason">%%1537:

%%1541: %%1801

%%1805

%%1811

D:(A;ID;0x1200a9;;;BU)

%%4423:

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>



Cabaré

Stratégies et GPO Audit windows 10 AD 2012R2 - 2016 - SYS 26- Cours - ver 2.6 - http://www.cabare.net Page 35 - Michel Cabaré -

STRATEGIE AUDIT RESSOURCE IMPRIMANTE

Savoir qui imprime :

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

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:

aramètres d	lu contrôle d'accès	pour HP Laser]	let 6P	<u>? ×</u>
Autorisations	Audit Propriétaire			
Entrées d'au	udit :			
Туре	Nom	Accès	Appliquer à	
Réussi	te Tout le monde	Imprimer	Cette imprimante et les documents	
Ajoute	r Supprin	her Afficher/I	Modifier	
				- 11
Cette entrée les objets et	e d'audit est définie dir pfants	ectement sur cet o	bjet. Cette entrée d'audit est héritée p	ar
ics objets ei	manks.			

onglet Sécurité / Avancées et onglet Audit...

Audit de l'entrée pour HP Laser] Objet	let 6P	3				
Nom : Tout le monde Modifier						
Appliquer à : Cette imprimante et les documents						
Accès :	Réussite	Échec				
Imprimer	$\mathbf{\nabla}$					
Gestion d'imprimantes						
Gestion des documents						
Autorisations de lecture	\checkmark					
Modifier les autorisations						
A die Kiese						



Stratégies et GPO Audit windows 10 AD 2012R2 - 2016 - SYS 26- Cours - ver 2.6 -

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 <u>sur la machine sur laquelle l'identification se fera</u>...

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 <u>ne sont pas disponibles</u> 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...





Pour obtenir dans le journal

Gestionnaire de serveur (SRV-2008)	Sécurité Nombre d	'événements : 72			Ac	
Ponctionnalités	Filtré : Journal: Security; Source: ; Mot clé: win:AuditFailure. Nombre d'événements : 2					
Diagnostics Observateur d'événements	Mots dés	Date et heure	Source	ID de l'évén Catégorie d		
Affichages personnalisés	🔒 Échec de l'audit	28/11/2009 13:16:49	Microsoft Wi	4771 Service d'au	1	
🖃 📫 Journaux Windows	🔒 Échec de l'audit	28/11/2009 13:16:41	Microsoft Wi	4771 Service d'au		
Application					-	
Installation	🛃 Propriétés de l	'événement - Événement 477	1, Microsoft W	indows security auditing.		
Événements transférés	Général Détails					
🗄 🔁 Journaux des applications et (
Abonnements						
OP Performance						
Gestionnaire de périphériques	Informations sur le compte :					
ID de sécurité : FORMATION\administrateur Stockage Nom du compte : administrateur						
	Journal :	Sécurité				
	Source :	Microsoft Windows security	Connecté : 2	28/11/2009 13:16:41		
	Événement :	4771	Catégorie :	Service d'authentification Kerberos	5	
	Niveau :	Information	Mots clés :	Échec de l'audit		



Stratégies et GPO Audit windows 10 AD 2012R2 - 2016 - SYS 26- Cours - ver 2.6 - http://www.cabare.net Page 38 - Michel Cabaré -