Henry Astafieff

Audit des serveurs windows

Suivre les étapes suivantes :

1. Ouvrez les stratégies de groupes locales, configuration ordinateur, paramètres windows, paramètres de sécurité, configuration avancée de la stratégie d'audit, accès à l'objet puis auditer le système de fichiers .

2. Cochez : Configurer les événements d'audit suivants et sélectionnez « Succès »

Configurer l'audit sur un fichier spécifique :

1. Ouvrez les propriétés du dossier avec le fichier

2. Allez paramètres de sécurité avancés et allez à l'onglet « Audit ».

3. Ajouter pour créer une nouvelle règle.

4. Définissez le principal à « Tout le monde » et cochez « Supprimer » et « Supprimer les sousdossiers et les fichiers ».

5. Testez en supprimant le fichier « document.txt » depuis un poste client. Un message d'audit correspondant devrait apparaître.



	C:\Parta	ge\Production	1		
Propriétaire :	Adminis	strateurs (LEAR	N\Administrateurs)	Modifier	
Autorisations	Partage	Audit	Accès effectif		
our obtenir de entrée et cliqu	es informations s uez sur Modifier (upplémentaire (si disponible).	s, double-cliquez su	r une entrée d'audit. Pour modifie	r une entrée d'audit, sélectionnez
Type P	: Principal		Accès	Hérité de	S'applique à
Ajouter	Supprime	r Affic	her		
Désactiver l' Remplacer to	héritage outes les entrées	d'audit des ob	jets enfants par des (entrées d'audit pouvant être hérité	es de cet objet Annuler Appliqu
Désectiver l' Remplacer tr incipal : Tou pe : Rem	héritage outes les entrées clemande Sélect saite	d'audit des ob	jets enfants par des o al	entrées d'audit pouvant être héritê	es de cet objet Annuler Appliqu
Désactiver l' Remplacer tr ncipal : Tou pe : Rem pplique à : Ce e	héritage outes les entrées tle monde Select suite dossier, les sous-dos	d'audit des ob ionnez un princip ssiers et les fichier	s v	entrées d'audit pouvant être hérité	es de cet objet
Désactiver l' Remplacer tr incipal: 1900 pe: Re- pplique à: Ce o torisations avanc	héritage outes les entrées thermonde Select asite dossier, les sous-dor	d'audit des ob ionnez un princip ssiers et les fichier	iets enfants par des e al s v	entrées d'audit pouvant être hérité	es de cet objet Annuler Appliqu Micher les extorisations de b
Désactiver l' Remplacer tr ncipel: Teu pe: Re- pplique à: Ce o torisations avanc	héritage outes les entrées tie mande Select ssite dossier, les sous-dor cés : trole total	d'audit des ob ionnez un princip ssiers et les fichier	si v	entrées d'audit pouvant être hérité	es de cet objet Annuler Appliqu Afficher les autorisations de b
Désactiver l' Remplacer tu ncipal: Jeu pei: Pei pplique à: Ces Aorisations avanc Com	héritage outes les entrées tie monde Select asite dossier, les sous-dor cés : trôle total cours du dotaiser/ent	d'audit des ob ionnez un princip ssiers et les fichier	s v	entrées d'audit pouvant être hérité	es de cet objet Annuler Appliqu Africher les autorisations de b
Désactiver l' Remplacer tr ncipal: low pe: Rem applique à: Ces dorisations avanc Loisi	héritage outes les entrées t le mande Select usite dossier, les sous-dor trôle total rours du dossier/ente e du dossier/ente	d'audit des ob ionnez un princip ssiers et les fichier icuter le fichier de données	il s v	entrées d'audit pouvant être hérité OK	es de cet objet Annuler Appliqu Afficher les autorisations de b
Désactiver l' Remplacer tr incipal : Teur pe : Rein pplique à Ce cr torisations avanc Late Attributer : Cen	héritage outes les entrées tie monde Select saite dossier, les sous-dos trole total cours du dossier/end e du dossier/enture bists de lecture	d'audit des ob ionnez un princip ssiers et les fichier icuter le fichier de données	al	entrées d'audit pouvant être hérité OK	es de cet objet Annuler Appliqu Afficher les autorisations de b
Désactiver l' Remplacer tr incipal: Jase pe: Pe: Pe: Atrisations evanc Con Pare Liste Liste Liste	héritage outes les entrées tie mande Select asite dossier, les sous-dor trôle total cours du dossier/ent e du dossier/ente e du dossier/enter ibuts de lecture une des atributs dir	d'audit des ob ionnes un princip ssiers et les fichier icuter le fichier de données endus	el	Attributs d'écriture	es de cet objet Annuler Appliqu Africher les autorisations de b
Désactiver l' Remplacer ta incipal : Taxa pe i Réa applique à : Ces atorisations avanc Con Parce Licto Catoria	héritage outes les entrées t le mande Select ssite dossier, les sous-do trôle total cours du dossier/end e du dossier/end e du dossier/end e du dossier/end e du dossier/end e du dossier/end e du dossier/end total cours du dossier/end e du dossi	d'audit des ob ionnes un princip ssiers et les fichier de données andus une de données	iets enfants par des e	Attributs d'écriture Cok Attributs d'écriture Écriture d'attributs étendus Suppression Autorisations de lecture Modifier les autorisations	es de cet objet Annuler Appliqu Afficher les autorisations de b
Désactiver l' Remplacer tr incipal : Tour pe i Bau spplique à : Ce cr con Lister Lister Con Con	héritage outes les entrées tle monde Sélect suite dossier, les sous-dos trôle total cours du dossier/lest a du dossier/lesture hare des attributs été tion de dossier/lest hare des attributs été	d'audit des ob ionnez un princip ssiers et les fichier de données endus ture de données	al	Autributs d'écriture Cok Cok Cok Cok Cok Cok	es de cet objet Annuler Appliqu Afficher les autorisations de b

Ajouter une condition

Steams Territre d'Aven	Actives						
Mata das	Date of heurs	Source	E de l'événement Catégorie de la té	de n	Securité		
Carola de l'autilit	16/05/2024 12:51:26	Microsoft Mindows security	4819 The System		a Duvir lejournal energietre.		
Surraix de l'autit	16/05/2024 12:48:52	Microsoft Windows security	4063 File System		P Diter und voe percennelisie		
Sociels de l'aveile	16/05/2534 15:41/21	Microsoft Windows security	4965 thite System		Importer une vue personnalisate		
Social de l'audit	14/06/2824 15:47:24	Microsoft Windows security	4900 Ella System		Manual Sciences		
Succes de l'autit	16/05/2024 15/47/21	Microsoft Windows security	4563 file System		officer a journal.		
Succes de l'euclit	16/05/2024 15:12:52	Microsoft Windows security	4719 Audit Policy Chan	QH .	Titler is journal actual		
Dutits de l'autit	16/15/2004 15/12/52	Microsoft Windows security	4719 Audit Policy Char	Qu.	- C Propriatio		
Touristo de l'anació	NUMBER OF THE PARTY OF THE PART	Microsoft Wondows tartady -	ACTU Auda Peley Char	5°	di fachanhan.		
Everyward 4670, Microsoft	×	fragister teas in intravants	enn				
fatated Bands	Initialize une titche it or jouenal.						
Contrast Contrast.	allchag						
Statue de seu un alije	IT American						
Décidente	and and a						
Now als com	E-memory and Microsoft Window	securi-					
Donaite da 1	Popoliti del'inversent						
	Chindre une tiche i ort Autoen	et.					
Orjet	LT freedom to determine the	in and					
Type d'objet:	Ind complete in eveneration	Acces.					
Nom de l'obje	de coper						
Didachandra: 00					15 Actualities		
leftern ations our le pro	Constant 1				Aide Aide		
D du process	ant: Osli						
1000							
Ineral Stratte							
Source : Microso	Window analy Committee H	6/05/008 15/1/26					
Education (1933	Categoria: 71	The System					
Norma: Informa	tion Mate-cile: Se	accès de l'audit					
(Minster) Pris	Column 0	C Lisson Incel					
The second secon	uraness. D						
Branchis Indonesi		Capital Information					
Openda: Informa	tions						

Pour créer une règle d'audit excluant certains utilisateurs :

1. Créez en excluant les utilisateurs « directeur » et « technicien informatique ».

2. Appliquez cette règle au dossier direction.

3. En tentant d'accéder au dossier Direction, un message doit apparaître dans le journal d'événements.