## VITAL Louis

Audit des serveurs Windows (système de fichiers)

Pour activer l'audit du système de fichiers sur un serveur Windows, suivez ces étapes :

1. Ouvrez les stratégies de groupes locales et naviguez jusqu'à « Configuration Ordinateur/Paramètres Windows/Paramètres de sécurité/Configuration avancée de la stratégie d'audit/Accès à l'objet/Auditer le système de fichiers ».

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

deligia Ordinateur local	Sous-catégorie	Einernents d'audit	Proprietan de l'Audher in postaren de Coblem
Configuration onlination	Auditer/Suplication générée	Non-configure	Treprinter de l'Austre la systeme de trevers
#aramétres du logiciel	R Auditer les services de certification	Non-configurii	Dratige Dolgaw
Perevaltas Windows	IR Auditer la partage de fichiers détaille	Non-configurati	
Multipe de resolution de nores	Audrier Te partage de lichiers	Non configuration	Author is systeme de Schiers
El scipts (demanage/anet)	R Auskterie systeme de Schien	Sector	
7 mil importantes deproyees	No Auditor to commission de la pristaforme de filtrage	Non configuration	
· In reserves to secure	The Auditor is relation to a second par is plateforme de filtr	Non configuration	
Strategies de comptes	Ri Auditer la manapolation de handle	Non configure	Configurer ins dedeaments d'audit subverte
Base day Windows Deliverity and Inscitores and	E Auditer Falget de novas	Non-confrigurat	Di Sarria
Stutiques du gestionnaire de lister de réseaux	Physicises of matters devicements of manins & Parkiet	Non-configurat	E) same
Studies de chimétique	Auditer te Registre	Non configure	C false
<ul> <li>Struttegies de restriction logicielle</li> </ul>	R Auditor Is stockage empythis	Non configure	
s 🔁 Strutségies de contrôlie de l'aquilication	R Audres SAM	New configuration	
a 🧏 Strategies de sécurité P sur Ordinateur lecal	C. Auditer in stratique d'araie, cant a faire reterminiques	Non-configurat	
- Configuration avanote de la dratégie d'audit			
🗸 🍂 Studiges d'audit système - Diget Rustège			
Connexion de compta			
Gertion du campte			
> III Sorvi détaille			
》 篇 Acob 05			
> Ja Ouviefferner la maine			
<ul> <li>Acob a fatter.</li> </ul>			
<ul> <li>A Changement de startégie</li> </ul>			
) []] UKkusture de precisige			
) III Systeme			
Aucht de l'accès globat aus objets			
Goo have on a datage			Contraction of the local division of the loc
Modelai diadministration			
Recently of the set			
a variation of other			

Pour configurer l'audit sur un fichier spécifique :

1. Ouvrez les propriétés du dossier contenant le fichier.

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

3. Cliquez sur « Ajouter » pour créer une nouvelle règle d'audit.

4. Définissez le principal à « Tout le monde » et cochez les options « Supprimer » et « Supprimer les sous-dossiers et les fichiers ».

5. Testez cette configuration en supprimant le fichier « document.txt » depuis un poste client. Vous devriez voir un message d'audit correspondant.

Général	Partage	Sécurité	Versions précédentes	Personnaliser	Classificat	tion
Nom de	l'objet :	C:\Partage	Production			
Noms de	groupes of	ou d'utilisate	eurs :			
S& Tou	ut le monde	e				
Sys Sys	tème	-				
👗 Adr	nin (Admin	)				
as Adr	ninistrateur	rs (LEARN\	Administrateurs)			
Pour mo	difier les au	utorisations.	cliquez sur Modifier.			
					- <b>-</b>	Modifier
		<b>-</b>		Δ. et	orieer F	Refuser
Autonsat	ions pour	l out le mon	de	Aut	onser r	heitusei
Contró	òle total					^
Contró Modifi	òle total cation					^
Contró Modifi Lectur	òle total cation re et exécu	ution			~	^
Contró Modifi Lectur Affich	òle total cation re et exécu age du cor	ution ntenu du do	ssier		✓ ✓	^
Contré Modifi Lectur Affich Lectur	òle total cation re et exécu age du cor re	ution ntenu du do	ssier		~ ~ ~	^
Contró Modifi Lectur Affichi Lectur Écritur	òle total ication re et exécu age du cor re re	ution ntenu du do	ssier		>>>	^
Contró Modifi Lectur Affich Lectur Écritur Autori	òle total cation re et exécu age du cor re re sations spé	ution ntenu du do éciales	ssier		$\langle \rangle \langle \rangle \langle \rangle$	~
Contré Modifi Lectur Affich: Lectur Écritur Autoris Pour les Avancé.	ile total cation re et exécu age du cor re re sations spé autorisatio	ution ntenu du do éciales ins spéciale:	ssier s et les paramètres avar	ncés, cliquez sur	~ ~ ~	∧ ∨ Wancé
Contró Modifi Lectur Affich Lectur Écritur Autoris Pour les Avancé.	ble total cation re et exécu age du cor re sations spé autorisatio	ution ntenu du do éciales Ins spéciale: contrôle d'a	ssier s et les paramètres avar locès et les autorisation:	ncés, cliquez sur	~ ~ ~	∧ vancé

Nom :	C:\Partag	e\Production	1		
Propriétaire :	Administ	ateurs (LEAR	N\Administrateurs)	Modifier	
Autorisations	Partage	Audit	Accès effectif		
Pour obtenir l'entrée et cli Entrées d'auc	des informations su quez sur Modifier (si lit :	pplémentaire disponible).	s, double-cliquez su	une entrée d'audit. Pour mod	ifier une entrée d'audit, sélectionnez
Туре	Principal		Accès	Hérité de	S'applique à
Ajouter Désactiver	Supprimer r l'héritage r toutes les entrées d	Affic audit des ob	her jets enfants par des e	ntrées d'audit pouvant être hé O <mark>K</mark>	ritées de cet objet Annuler Applique
Principal : Type : S'applique à :	Tout le monde Sélecti Réussite Ce dossier, les sous-dos	onnez un princij siers et les fichie	ers v		
Autorisations an	vancées : Contrôle total Parcours du dossier/exé Liste du dossier/lecture d Attributs de lecture Lecture des attributs éte Création de fichier/écrits Création de dossier/ajou s paramètres d'audit uni	uter le fichier Je données ndus Ire de données t de données quement aux ob	ojets et/ou aux conteneu	Attributs d'écriture     Écriture d'attributs étendus     Suppression de sous-dossier e     Suppression     Autorisations de lecture     Modifier les autorisations     Appropriation	Afficher les autorisations de b & fichier Effacer tout
Ajoutez une cor Ajouter une cor	ndition pour limiter l'éte	ndue de cette ei	ntrée d'audit. Les événem	ents de sécurité ne seront enregistré:	s que si les conditions sont remplies.

enements (Loc Securité Nombre d'évén	ements : 24 689			Actions
Mata cita	Cole at hours	Source	ID de l'événement Catégorie de la têche	<ul> <li>Séculté</li> </ul>
Ho d'administre Succès de l'audit	16/05/2024 12:51:26	Microsoft Windows security	4839 File System	🧉 Duvrir le journal enregistré
sts de la page d 🤍 Succès de l'audit	16/05/2024 13:4E 52	Microsoft Windows security	4963 File System	Criter une vue personnaliste
dows Succes de Faudit	16/05/2884 18/47/21	Microsoft Windows security	4908 File System	Importer une vue personnalisée
on Succito de l'analit	16/05/2024 13:47.21	Microsoft Windows security	4600 File Systems	The second
Succès de l'audit	16/05/2024 13:47:21	Microsoft Windows security	4963 File System	theor is journe
Succès de l'audit	16/05/2024 13:12:52	Microsoft Windows security	4719 Audit Policy Change	Fiber la journal actual
Succes de l'audit	16/05/2024 13:12:52	Microsoft Windows security	4719 Audit Policy Change	Proprietais
analizations at	16/05/2028 13:12:52	Microsoft Windows security	4719 Audit Policy Change	<ul> <li>OB Rechercher</li> </ul>
Environment 4550. USe small	Wenters security authing.			X G framinitations in interaction
				- Bill International Contraction
Général Details				Joindre une tiche a ce journal.
				Affichage
Un handle vers on obje	t a été élemanélé dans un but de suppression.		^	Actualiser
Sujet:				1 Aide
D de sécurité	: LEARMicristan			E-instant 1995 Manual Western or
Domaine du c	ompte : LEARN			EVENENCE AND
Difeestat	de session : 0x276094			Proprietes de l'evenement
Chiefe				Joindre une tiche à cet événement
Serveur de l'ol	tjet: Security			Enregistrer les événements sélection
Type d'objet :	Fie			Copier
D do banding	<ol> <li>Chratage/Production/Docutecument.td 5-0</li> </ol>			R. Arturbar
				A ALLER A
Informations sur le pro-	C REGULES 1			Aide Aide
D du process	11:04		v	
Jacobia Singela				
	bill design of the second second second			
Source: Marchae	Preventions security Convector Techy2024	141124		
Evenement: 4659	Catégorie : File System	•		
Niveau: Informat	tion Mate-clés : Succès del	l'audit		
Utilisateur: IVA	Ordinateur: DCUsand	local		
Onundary Information	times.			
opena. Increa	or or the			

Pour créer une règle d'audit excluant certains utilisateurs :

1. Créez une nouvelle règle d'audit 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 approprié devrait apparaître dans le journal d'événements.