ManageEngine
ADAudit Plus

Les **8** ID d'événements de **sécurité Windows** les plus critiques

Table des matières

Le journal de sécurité Windows

Le journal de sécurité Windows, que vous trouverez dans l'Observateur d'événements, enregistre les actions critiques des utilisateurs, telles que les ouvertures et fermetures de session, la gestion des comptes, l'accès aux objets, et plus encore.

Microsoft décrit le journal de sécurité Windows comme «votre meilleure et dernière défense», et ce à juste titre. Le journal de sécurité permet de détecter les problèmes de sécurité potentiels, de garantir la responsabilité des utilisateurs et de servir de preuve en cas de violation de la sécurité.

Qu'est-ce qui rend un événement de sécurité Windows critique ?

Parmi la multitude d'événements de sécurité Windows, les rares qui peuvent être considérés comme critiques peuvent être classés en deux groupes :

1. Les événements dont l'occurrence unique indique une activité malveillante. Par exemple, un compte utilisateur final normal ajouté de manière inattendue à un groupe de sécurité sensible.
2. Les événements dont l'occurrence successive au-dessus d'une ligne de base acceptée indique une activité malveillante. Par exemple, un nombre anormalement élevé d'échecs de connexion.

Les 8 ID d'événements de sécurité Windows les plus critiques

Série	Catégorie	ID d'événement et description	Raisons de la surveillance (liste non exhaustive)
(1) & (2)	**Connexion et déconnexion**	**4624** (Connexion réussie)	• Détecter les activités anormales et éventuellement non autorisées d'un utilisateur, comme une connexion à partir d'un compte inactif ou restreint, des utilisateurs se connectant en dehors des heures de travail habituelles, des connexions simultanées à de nombreuses ressources, etc. • Pour obtenir des informations sur le comportement des utilisateurs, comme leur présence, leurs heures de travail, etc.
		4625 (Échec de connexion)	• Détecter les éventuelles attaques par force brute, par dictionnaire ou par d'autres moyens de deviner un mot de passe, qui se caractérisent par un pic soudain d'échecs de connexion. • Pour arriver à un point de repère concernant le paramètre de la stratégie du seuil de verrouillage de comptes.
(3), (4) & (5)	**Gestion du compte**	**4728** (Membre ajouté à un groupe global de sécurité) **4732** (Membre ajouté au groupe local de sécurité) **4756** (Membre ajouté au groupe universel de sécurité)	• Pour s'assurer que l'appartenance aux groupes des utilisateurs privilégiés, qui détiennent les «clés du royaume», est examinée régulièrement. Ceci est particulièrement vrai pour les ajouts de membres aux groupes de sécurité. • Pour détecter les abus de privilèges par les utilisateurs responsables d'ajouts non autorisés. • Pour détecter les ajouts accidentels.

(6)	**Journal des événements**	**1102** (Journal effacé) (Il est également possible de désactiver le service journal des événements, en conséquence, les journaux ne seront pas enregistrés. Ceci est fait par la stratégie d'audit du système, auquel cas l'événement **4719** est enregistré.)	• Pour repérer les utilisateurs ayant des intentions malveillantes, tels que ceux responsables de la falsification des journaux d'événements.
(7)	**Gestion du compte**	**4740** (Compte utilisateur bloqué)	• Détecter les éventuelles attaques par force brute, par dictionnaire ou par d'autres moyens de deviner un mot de passe, qui se caractérisent par un pic soudain d'échecs de connexion. • Atténuer l'impact des utilisateurs légitimes qui sont bloqués et ne peuvent pas effectuer leur travail.
(8)	**Accès à l'objet**	**4663** (Tentative d'accès à un objet)	• Pour détecter les tentatives non autorisées d'accès aux fichiers et aux dossiers.

Sécurisation de l'Active Directory

Avant tout, vous devez configurer votre stratégie d'audit pour que Windows puisse enregistrer les événements pertinents dans le journal de sécurité.
Ensuite, vous devez regrouper et analyser les journaux collectés, puis traduire ces résultats en informations exploitables, comme des rapports et des alertes. L'utilisation d'outils natifs et de scripts PowerShell pour accomplir ces tâches exige une expertise et beaucoup de temps. Pour effectuer le travail rapidement et efficacement, un outil tiers est vraiment indispensable.

Grâce à des rapports détaillés, des alertes en temps réel et des affichages graphiques, ADAudit Plus simplifie la surveillance continue des ouvertures et fermetures de session, des changements d'appartenance à un groupe, de l'effacement des journaux d'événements, des verrouillages de comptes, des serveurs de fichiers et bien plus encore dans votre Active Directory, vos serveurs membres et vos postes de travail.

Note

Bien que le plus grand soin ait été apporté à la préparation de ce document, nous ne donnons aucune garantie quant à celui-ci, notamment quant à l'exactitude des informations qu'il contient.