

Présentation

# ADAudit Plus

novembre 2023

## **Présentation ADAudit Plus**

### **1. Audit Windows Active Directory en temps réel**

En temps réel, assurez un audit, un suivi et un reporting des ressources vitales du réseau comme les contrôleurs de domaine avec une information complète sur les modifications des objets AD (utilisateurs, groupes, ordinateurs, GPO, OU, DNS, schéma AD et configuration) et plus de 200 rapports graphiques détaillés sur les différents événements et des alertes par e-mail.

#### **1.1 Menaces internes**

Décelez les signes d'une menace interne. Pour un compte donné, obtenez une synthèse de trois pistes d'audit : activité des utilisateurs dans AD, rapports sur l'accès et rapports sur les modifications d'autorisations. La piste d'audit offre un contexte qui facilite l'identification interne. Vous déterminez aussi instantanément les ordinateurs compromis par un utilisateur et les modifications.

#### **1.2 Connexion utilisateur**

Suivez en temps réel les activités de connexion des utilisateurs à des contrôleurs de domaine avec des rapports d'audit préconfigurés et des alertes par e-mail. Les rapports d'audit garantissent que l'administrateur connaît la raison des échecs de connexion des utilisateurs, l'historique de connexion, les opérations des services de terminal et l'activité de connexion récente des utilisateurs sur le réseau des serveurs Windows.

#### **1.3 Conformité**

Les PME ou les grandes entreprises doivent respecter des normes de conformité sectorielles de type SOX, HIPAA, GLBA, PCI-DSS, FISMA... Nos rapports préconfigurés et alertes de conformité en temps réel assurent un audit réseau en continu. La procédure standard utilise des rapports de sécurité périodiques et des alertes par e-mail.

#### **1.4 Rapports et alertes**

Choisissez parmi plus de 200 rapports d'audit préconfigurés planifiables, créez des rapports personnalisés, définissez des rapports par profil et générez des rapports à partir des données archivées pour l'investigation. En temps réel, suivez les modifications des objets Windows AD (utilisateur, OU, groupe, GPO, ordinateur, schéma, DNS et système) et recevez des alertes par e-mail sur les événements d'accès réseau ou de modification sans autorisation.

### 1.5 Archivage de données

Exécutez un archivage périodique des données des événements audités pour gagner de l'espace disque. Affichez des rapports sur les anciens événements comme l'historique de connexion des utilisateurs Active Directory, l'historique des modifications de mot de passe et autres à partir des données d'audit archivées pour l'analyse des ordinateurs ou la conformité. Vous pouvez exporter les rapports d'audit aux formats XLS, CSV, PDF et HTML.

### 1.6 Configuration GPO

Effectuez un audit et un reporting sur les modifications GPO dans Active Directory et les serveurs Windows. Assurez un suivi avancé approfondi des anciennes et nouvelles valeurs de configuration des objets stratégie de groupe, des modifications des paramètres et des stratégies de mot de passe. Respectez les exigences réglementaires en matière de sécurité réseau et diverses normes de conformité.

## **2. Audit des connexions/déconnexions Windows**

Vérifiez les heures de connexion/déconnexion des postes de travail des utilisateurs critiques avec les durées, les échecs et l'historique de connexion, ainsi que l'activité des services de terminal. Consultez et planifiez des rapports graphiques avec des alertes par e-mail pour une analyse périodique et une réaction rapide en cas de menaces de sécurité.

### **2.1 Connexion/déconnexion**

L'audit des postes de travail des utilisateurs Windows indique l'heure exacte de connexion et de déconnexion pour vérifier rapidement le statut de l'utilisateur lors d'une tentative d'accès non autorisé sur le poste de travail. De plus, les rapports et les alertes par e-mail instantanées informent sur la durée de connexion, les échecs et l'activité des services de terminal.

### **2.2 Conformité**

Les PME ou les grandes entreprises doivent respecter des normes de conformité sectorielles de type SOX, HIPAA, GLBA, PCI-DSS, FISMA... Nos rapports préconfigurés et alertes de conformité assurent un audit réseau en continu. La procédure standard utilise des rapports de sécurité périodiques et des alertes par e-mail.

### **2.3 Archivage de données**

Dans le produit, exécutez un archivage périodique des données des événements audités pour gagner de l'espace disque. Affichez des rapports sur les anciens événements comme l'historique de connexion des utilisateurs des postes de travail, les échecs de connexion, l'activité des services de terminal et autres à partir des données d'audit archivées pour l'analyse des ordinateurs ou la conformité. Vous pouvez exporter les rapports d'audit aux formats XLS, CSV, PDF et HTML.

### **2.4 Rapports et alertes**

Choisissez parmi les nombreux rapports d'audit préconfigurés planifiables pour les postes de travail avec de multiples attributs de filtre, créez des rapports personnalisés, définissez des rapports par profil et générez des rapports à partir des données archivées pour l'investigation. Suivez l'activité des postes de travail Windows et recevez des alertes par e-mail sur les événements d'accès réseau non autorisé.

### **2.5 Rapports globaux des postes de travail**

Liste complète sous la catégorie des rapports des postes de travail. Les administrateurs/auditeurs peuvent ainsi suivre et contrôler les événements des

postes de travail sous chaque angle possible avec de nombreux rapports graphiques faciles à comprendre.

### **3. Audit des serveurs de fichiers Windows**

Suivez en toute sécurité la création, la modification et la suppression de fichiers via un accès autorisé ou non, avec analyse détaillée des modifications de sécurité et d'autorisation apportées aux documents dans leur structure de fichiers/dossiers et les partages.

#### **3.1 Serveurs de fichiers**

L'audit des serveurs de fichiers Windows dans un environnement Microsoft Server permet d'assurer un suivi fiable, d'afficher des rapports préconfigurés ou d'obtenir des alertes par e-mail instantanées pour les modifications, l'accès aux documents, les changements de structure de fichiers/dossiers, les partages et les autorisations d'accès.

#### **3.2 Autorisations d'accès**

Vérifiez les paramètres de sécurité pour tout savoir sur vos partages réseau dans Windows. Gardez une trace de chaque modification de fichier/dossier, de partage et d'autorisation. Suivez les modifications discrétionnaires et SACL avec le détail des anciennes et nouvelles valeurs des attributs de sécurité.

#### **3.3 Clusters de basculement**

Auditez et suivez les clusters de basculement des serveurs de fichiers Windows. Suivez les partages de cluster des utilisateurs et les autorisations d'accès. En outre, auditez la sécurité des partages de fichiers avec les rapports planifiables et les alertes par e-mail instantanées.

#### **3.4 Filers NetApp**

L'audit des filers NetApp pour Windows permet aux administrateurs de suivre chaque création, modification ou suppression de fichier/dossier Windows et NetApp Filer CIFS, ainsi que les changements de paramètres et d'autorisations. Surveillez en temps réel grâce aux rapports préconfigurés et aux alertes par e-mail les atteintes à la sécurité réseau et l'accès aux objets critiques.

#### **3.5 Serveurs EMC**

Vérifiez les modifications des partages de fichiers EMC (VNX/VNXe/Celerra) avec les rapports d'audit classés en catégorie par fichier, serveur, utilisateur et partage. Obtenez des rapports personnalisés et documentez les changements des fichiers et des dossiers. Contrôlez l'accès, les partages et les autorisations. Exportez des rapports pour l'analyse de sécurité et le respect des exigences de conformité.

### 3.6 Tous les rapports sur les serveurs de fichiers

Consultez tous les rapports sous la catégorie serveur de fichiers. Les administrateurs/auditeurs peuvent ainsi suivre et contrôler les événements de sécurité sur les serveurs de fichiers Windows, d'accès et de modification sous chaque angle possible avec de nombreux rapports graphiques faciles à comprendre.

## **4/ Audit des serveurs Windows**

Suivez les connexions/déconnexions et planifiez le suivi d'événements comme la connexion RADIUS, l'activité des services de terminal, la durée et l'historique des connexions. Vous pouvez contrôler les processus d'audit via le suivi des tâches planifiées Windows.

### **4.1 Serveurs Windows**

L'audit des serveurs membres Windows permet d'analyser l'activité de connexion/déconnexion et les services Terminal Server essentiels, dont les modifications de stratégie avec des tâches planifiées, la gestion des objets, les événements système, les rapports de suivi de processus et les alertes par e-mail.

### **4.2 Audit des imprimantes**

Les administrateurs peuvent vérifier, analyser et suivre de façon centralisée tous les fichiers imprimés via le réseau Windows Server, avec des rapports complets sur l'utilisation des imprimantes, les travaux récents, les utilisateurs/ imprimantes pour une meilleure sécurité et conformité SOX ou HIPAA.

### **4.3 Analyse d'intégrité des fichiers**

Cette fonction permet d'analyser les modifications apportées aux fichiers du système Windows, de configuration, de programme (journal, audit, texte, exécutable, Web, configuration, base de données), aux attributs (dll, exe et autres fichiers système) et aux dossiers. On peut aussi planifier des rapports réguliers au format XLS, HTML, PDF ou CSV envoyés par e-mail pour l'analyse réseau.

### **4.4 Conformité**

Les petites, moyennes ou grandes entreprises doivent se conformer à des normes sectorielles comme SOX, HIPAA, GLBA, PCI-DSS ou FISMA. Des rapports et des alertes préconfigurés sur la conformité assurent un audit de sécurité permanent du réseau dans le cadre des procédures standards.

### **4.5 Rapports et alertes**

Vérifiez les serveurs Windows en affichant des rapports d'audit préconfigurés avec des attributs de filtre et suivez la connexion/déconnexion des serveurs membres Windows. Bénéficiez de rapports sur l'activité des services Terminal Server, suivez les processus des serveurs et analysez les tâches planifiées avec des rapports et des alertes.

### **4.6 Ensemble des rapports Windows Server**

Affichez tous les rapports dans la catégorie des rapports Windows Server. De nombreux rapports graphiques faciles à comprendre aident les administrateurs/auditeurs à vérifier et analyser la sécurité des serveurs Windows,

et à suivre les processus et les événements système. On peut afficher les rapports pendant et en dehors des heures de bureau.

## **5/ Exemples de rapports**

### **5.1 Activité de connexion sur les serveurs membres et les postes de travail**

- Vérifier l'absentéisme et la présence des employés dans un intervalle d'audit donné/chaque mois.
- Déterminer le nombre total des utilisateurs qui ont accès au réseau Active Directory à un instant donné.
- Identifier les utilisateurs qui ont accès à des postes de travail ou des contrôleurs de domaine via un ordinateur en réseau distant.
- Déterminer les heures de connexion de pointe pour tous les utilisateurs dans le domaine.
- Savoir qui a effectué la dernière connexion à un ordinateur du domaine essentiel.
- Identifier si un utilisateur (malveillant) tente de se connecter à des machines pour lesquelles il ne possède pas de privilèges. (Par exemple : la connexion à un contrôleur de domaine ou un serveur membre dans Active Directory exige des privilèges élevés).
- Afficher en intégralité l'historique de connexion d'un utilisateur dans le domaine. Vous disposez ainsi d'une preuve quand vous interrogez un employé suspect avec les objets de domaine Active Directory, comme les ordinateurs, les groupes et d'autres comptes d'utilisateurs, que l'employé a administré, a modifié ou auxquels il a accédé pendant sa collaboration.

Outre ceux déjà énumérés, il existe de nombreux autres besoins pratiques dans un réseau Active Directory qui exigent des données d'audit sur les connexions aux comptes du domaine. Les rapports sur les connexions aux comptes d'ADAudit Plus sont utiles pour relever les défis en termes d'audit.

La solution offre une série de rapports prédéfinis en temps réel pour apporter des réponses aux questions en matière d'audit des connexions dans le format souhaité et améliore le contrôle Active Directory. Les rapports personnalisés rendent la solution encore plus intéressante. Par exemple, vous pouvez définir une action de connexion et l'examiner sous forme d'un rapport.

Raisons des lacunes de l'audit Active Directory natif en termes de connexion des utilisateurs

Chaque événement de connexion AD est enregistré en continu dans les journaux de sécurité des contrôleurs de domaine Active Directory. Les données enregistrées dans les journaux de sécurité natifs des contrôleurs de domaine Active Directory :

- Demandent une expertise pour leur compréhension, car il faut analyser des codes d'événement particuliers et leur corrélation à une action de connexion.
- forment un gros volume, chaque activité de connexion sur/par un objet Active Directory étant consignée en continu dans le contrôleur de domaine, d'où l'accumulation d'un énorme volume de données dans les journaux d'événements.

- présentent un accès restreint, le contrôleur de domaine étant un élément clé de l'infrastructure Active Directory et son accès limité à certains utilisateurs administratifs.

D'autres limitations de l'audit Active Directory natif incluent l'incapacité pour les utilisateurs non administratifs comme les auditeurs, les gestionnaires et le personnel des ressources humaines de suivre une action de connexion donnée.

Certains événements de connexion cruciaux comme la connexion à un contrôleur de domaine ou un serveur membre nécessitent des alertes immédiates ou un suivi continu. Bien qu'enregistrées, les informations essentielles ne sont pas différenciées ou regroupées par rapport à un journal d'événements normal et présentent un risque de négligence accru.

- Audit Active Directory
- Suivi des actions de gestion des utilisateurs
- Rapports d'audit de gestion des utilisateurs
- Audit des modifications d'autorisations Active Directory
- Analyse de verrouillage de compte
- Solution d'audit SIEM
- Rapports d'audit des groupes Active Directory
- Heures de travail des employés
- Analyse AD en temps réel
- Suivi des actions de connexion des utilisateurs
- Rapports d'audit des connexions des utilisateurs
- Audit des modifications GPO
- Rapports d'audit avancé des GPO
- Modifications d'attributs AD nouveaux/anciens
- Alertes Active Directory et messages de notification
- Audit des journaux de sécurité Windows
- Audit LAPS Active Directory
- Audit de sécurité Active Directory
- Détection des menaces internes
- Planification de rapports sur les modifications Active Directory
- Rapports à partir de données archivées
- Audit de schéma DNS Windows
- Audit du stockage amovible
- Rapports d'audit de conformité
- Rapports d'audit des modifications AD en temps réel
- Intégration SIEM
- Audit Azure AD
- Outil d'examen des comptes verrouillés
- Analyse du comportement utilisateur (UBA)

## 5.2 Rapports d'audit de connexion des utilisateurs dans ADAudit Plus

### 5.2.1 Rapport sur les échecs de connexion

Ce rapport fournit des informations sur les échecs de connexion et leur raison au cours d'une période donnée. Plusieurs tentatives de connexion à des comptes d'utilisateurs qui ont échoué pendant cette période sont signalées. Les administrateurs disposent ainsi d'informations sur d'éventuelles attaques sur des comptes aux risques d'intrusion. Le rapport comprend les détails des échecs de connexion avec le moment de l'événement, le compte concerné et les causes possibles.

Les raisons d'un échec de connexion peuvent être graves comme un nom d'utilisateur incorrect ou un mauvais mot de passe, avec un risque d'attaques. Voici des causes nécessitant l'attention de l'administrateur : mot de passe expiré, compte désactivé/expiré/bloqué ou l'administrateur doit réinitialiser le mot de passe du compte. Le rapport signale aussi d'autres raisons comme une restriction d'accès par poste de travail, un défaut de réplication du compte d'un nouvel ordinateur, un nom d'ordinateur pré-Windows 2000 ou un problème de synchronisation entre l'heure du poste de travail et celle des contrôleurs de domaine.

Une représentation graphique du **nombre d'échecs de connexion par raison** aide les administrateurs à prendre des décisions rapides et à agir efficacement.

### 5.2.2 Activité de connexion aux contrôleurs de domaine

Les contrôleurs de domaine sont les éléments clés centraux de l'infrastructure Active Directory pour effectuer des modifications. La connexion à un contrôleur de domaine est réservée aux utilisateurs privilégiés ou administrateurs. Des informations complètes sur les tentatives de connexion effectuées par d'autres utilisateurs permettent aux administrateurs de prendre des mesures correctives fondées. ADAudit Plus fournit des détails sur tous les utilisateurs qui se sont connectés à un contrôleur de domaine donné. Le rapport comprend des détails comme l'heure de connexion, le nom de la machine à l'origine de la connexion d'un utilisateur, la réussite ou l'échec de la tentative de connexion et la raison de l'échec éventuel.

### 5.2.3 Activité de connexion aux serveurs membres et aux postes de travail

Le rapport sur l'activité de connexion aux serveurs membres et aux postes de travail fournit des informations sur la connexion des utilisateurs à certains serveurs membres ou postes de travail, respectivement. Les deux rapports fonctionnent

comme celui sur l'activité de connexion aux contrôleurs de domaine, ce qui facilite le traitement et la compréhension des informations.

#### 5.2.4 Activité de connexion des utilisateurs

Ce rapport fournit des informations d'audit sur l'historique de connexion complet à des serveurs ou des postes de travail auxquels accède un utilisateur du domaine donné. L'historique de connexion d'un objet utilisateur est très important pour comprendre le profil de connexion d'un utilisateur donné. Dans certains cas, il procure une trace enregistrée de l'activité d'un utilisateur pour des auditeurs ou responsables.

#### 5.2.5 Activité de connexion récente des utilisateurs

Un administrateur système s'interroge ou se préoccupe au sujet d'anomalies dans l'utilisation du réseau par des utilisateurs. L'échec d'une tentative de connexion est un signe ou une mesure pour déceler une anomalie. Le rapport sur l'activité de connexion récente des utilisateurs répertorie toutes les opérations de connexion ayant réussi ou échoué au cours de la période choisie. Il indique également la raison d'un échec de connexion pour aider à prendre des mesures correctives.

Ce rapport permet d'afficher une liste des utilisateurs connectés avec succès au réseau un jour donné, à une date choisie ou au cours d'une période donnée.

#### 5.2.6 Dernière connexion sur des postes de travail

Ce rapport fournit des informations sur l'heure de la dernière connexion à un poste de travail ou un ordinateur par tous les utilisateurs qui se sont connectés avec succès un jour donné. Ce rapport permet, par exemple, de déterminer l'absentéisme ou l'état de disponibilité actuel des utilisateurs dans l'entreprise.

#### 5.2.7 Suivi de connexion RADIUS sur des ordinateurs

Vérifiez l'accès réseau RADIUS (Remote Authentication Dial-In User Service) par des utilisateurs connectés sur des ordinateurs distants. Des rapports sur les échecs de connexion RADIUS (NPS) et l'historique de connexion RADIUS (NPS) pour les utilisateurs connectés à distance permettent de contrôler toute l'authentification RADIUS dans Active Directory. Veuillez noter que seules sont prises en charge actuellement les activités de connexion RADIUS via le serveur NPS (serveur de stratégie réseau, Windows Server 2008).

Vérifiez les dates/heures de connexion/déconnexion sur des postes de travail d'utilisateurs sensibles avec la durée. Affichez et planifiez des rapports graphiques avec des messages de notification pour une analyse périodique et une réaction rapide en cas de menaces de sécurité.

- Audit des postes de travail Windows
- Rapports d'audit et alertes instantanées
- Suivi de l'activité de connexion utilisateur
- Audit des connexions/déconnexions utilisateur locales
- Rapports d'audit de conformité
- Heures de travail des employés
- Rapports sur les échecs de connexion
- Audit des journaux de sécurité et des événements système
- Audit du stockage amovible
- Analyse d'intégrité des fichiers
- Audit des tâches et des processus planifiés
- Rapports d'audit des modifications de tous les postes de travail Windows

### 5.3 Audit des serveurs de fichiers Windows

Suivez en toute sécurité la création, la modification et la suppression de fichiers depuis un accès autorisé ou pas, avec une analyse détaillée des modifications des documents dans leur structure de fichiers et de dossiers, des partages et des autorisations.

- Audit des serveurs de fichiers Windows
- Autorisations de modification et d'accès
- Audit des systèmes de stockage NetApp
- Audit des serveurs de fichiers EMC
- Rapports et alertes planifiés
- Audit des clusters de serveur de fichiers
- Rapports d'audit de conformité
- Rapports d'audit de toutes les modifications des serveurs de fichiers Windows

## 5.4 Audit des serveurs Windows

Suivez la connexion/déconnexion, planifiez le suivi d'événements comme la connexion RADIUS, l'activité des services Terminal Server, la durée de connexion et l'historique de connexion. On peut contrôler l'audit des processus connexes en suivant les tâches planifiées Windows.

- Audit des serveurs membres Windows
- Rapports d'audit et alertes instantanées
- Audit des connexions/déconnexions d'utilisateur locales
- Audit des journaux de sécurité et des événements système
- Audit des tâches et des processus planifiés
- Audit des stratégies locales et des droits d'utilisateurs
- Contrôle d'intégrité des fichiers
- Audit ADFS
- Audit des imprimantes
- Rapports d'audit de conformité
- Rapports d'audit de toutes les modifications des serveurs membres