LAZAR SOFT

Expert Partner ManageEngine

FICHE SOLUTION · GESTION DES ACCÈS ET DES IDENTITÉS (IAM)

# ManageEngine ADAudit Plus

# L'outil d'audit fondé sur l'analyse comportementale.

Protégez votre entreprise contre les menaces internes et les cyberattaques en auditant votre Active Directory, vos serveurs de fichiers, vos serveurs Windows et vos postes de travail — qui a fait quoi, quand, depuis où, et avec quelle valeur avant et après.

Contrôleurs de domaine | Tenants Azure AD | Serveurs Windows | Serveurs de fichiers Windows | Serveurs NAS | Postes de travail

TROIS ÉDITIONS · LICENCE PAR MODULE

**Gratuite · Standard · Professionnelle**

Tarif éditeur **à partir de 595 €/an** pour les contrôleurs de domaine — détail complet en page 5.

| 250+ | UBA | 6 | E-mail · SMS |
|---|---|---|---|
| RAPPORTS D'AUDIT ET DE CONFORMITÉ | ANALYSE DU COMPORTEMENT DES UTILISATEURS | MODULES SOUS LICENCE | ALERTES INSTANTANÉES |

**LAZAR SOFT**
Distributeur & intégrateur ManageEngine en France

TÉLÉPHONE
+33 (0)1 76 21 60 43

E-MAIL
sales@lazarsoft.com

# Chaque changement, tracé. Chaque écart, signalé.

## Ce qu'est ADAudit Plus

ADAudit Plus est un auditeur de changements piloté par l'analyse du comportement des utilisateurs (UBA), qui protège votre Active Directory, vos serveurs Windows, vos serveurs de fichiers et vos postes de travail, tout en assurant conformité et sécurité.

Là où un journal d'événements brut vous laisse face à des milliers de lignes, ADAudit Plus restitue l'information sous une forme exploitable : qui a modifié quoi, quand, depuis quelle machine, et quelle était la valeur de l'attribut avant et après. L'analyse comportementale établit ensuite la normale de chaque utilisateur et signale les écarts.

## Ce que la solution rend possible

- Détecter les menaces internes et les comportements anormaux avant qu'ils ne deviennent un incident.
- Repérer les signes précurseurs d'une attaque par rançongiciel et déclencher une réponse automatisée.
- Répondre aux exigences de conformité HIPAA, RGPD, PCI DSS, SOX, GLBA, FISMA et ISO 27001.
- Identifier en quelques minutes la source d'un verrouillage de compte récurrent.
- Conserver une piste d'audit exploitable en analyse forensique après incident.

### MODULES SOUS LICENCE

- Contrôleurs de domaine
- Tenants Azure AD
- Serveurs Windows
- Serveurs de fichiers Windows
- Serveurs NAS
- Postes de travail

### EXIGENCES SYSTÈME

**Processeur** 4 cœurs · **RAM** 8 Go · **Disque** 50 Go
**Navigateurs** Mozilla Firefox, Google Chrome, Microsoft Edge

## Le périmètre couvert par la plateforme — 10 domaines d'audit

### ANNUAIRE

- Modifications dans Active Directory et Azure AD
- Paramètres de stratégie de groupe (GPO)
- Utilisateurs à privilèges

### FICHIERS ET SERVEURS

- Modifications de fichiers
- Serveurs Windows

### ACCÈS ET COMPTES

- Connexions et déconnexions
- Verrouillages de comptes
- Activité des employés

### MENACES ET CONFORMITÉ

- Malwares et menaces internes
- Rapports de conformité

Le détail de chaque domaine figure aux pages 3 et 4.

## Plateformes prises en charge

### SERVEURS ET POSTES

- Windows Server 2003/2003 R2 · 2008/2008 R2 · 2012/2012 R2 · 2016/2016 R2 · 2019
- Postes de travail Windows XP et versions ultérieures

### SERVEURS DE FICHIERS ET NAS

- Windows File Server 2003 et versions ultérieures
- EMC VNX, VNXe, Celerra, Unity, Isilon · Synology DSM 5.0+ · NetApp Data ONTAP 7.2+ (filer) et 8.2.1+ (cluster) · Hitachi NAS 13.2+ · Huawei OceanStor V5 et 9000 V5

### AUTRES COMPOSANTS ET NAVIGATEURS

- ADFS 2.0 et versions ultérieures · PowerShell 4.0 ou 5.0
- Mozilla Firefox, Google Chrome, Microsoft Edge

# L'annuaire, les fichiers et les serveurs

## Audit des modifications dans Active Directory et Azure AD

CONTRÔLEURS DE DOMAINE · TENANTS AZURE AD

- **Auditez les modifications d'AD** — suivez les changements apportés aux unités d'organisation, aux utilisateurs, aux groupes, aux ordinateurs, aux groupes administratifs et aux autres objets AD.
- **Retracez l'historique des modifications des objets** — recevez des rapports d'audit détaillés indiquant les anciennes et les nouvelles valeurs des attributs modifiés.
- **Surveillez les modifications DNS et du schéma** — visibilité sur l'ajout, la modification et la suppression des nœuds et zones DNS ; surveillance des changements de schéma et de configuration d'Active Directory.
- **Suivez les changements de permissions AD** — affichez toutes les modifications des autorisations, notamment celles appliquées au niveau du domaine, des OU, du schéma, de la configuration et du DNS.
- **Auditez la gestion des comptes utilisateurs** — création, suppression et modification des utilisateurs, réinitialisations de mot de passe et autres actions liées à la gestion des comptes.
- **Surveillez les environnements AD hybrides** — vue unifiée de toutes les activités sur vos environnements Active Directory locaux et Azure AD, avec des alertes pour les événements critiques.

## Surveillance des modifications de fichiers

SERVEURS DE FICHIERS WINDOWS · NAS

- **Surveillez les accès aux fichiers et dossiers** — suivez en temps réel les tentatives d'accès réussies ou échouées : création, lecture, suppression, modification, copie/collage et déplacement.
- **Auditez les changements de permissions** — modifications des autorisations NTFS et de partage, avec le détail des anciennes et nouvelles valeurs.
- **Surveillez l'intégrité des fichiers** — rapports détaillés sur toutes les modifications apportées aux fichiers système et aux programmes critiques, avec alertes en cas d'activité suspecte.
- **Rapports sur les fichiers partagés** — suivez chaque accès et chaque modification dans votre domaine, avec le détail de qui a accédé à quoi, quand et depuis où.
- **Simplifiez les audits de conformité** — rapports prêts à l'emploi pour HIPAA, RGPD, FISMA, PCI DSS, SOX, GLBA et ISO 27001.
- **Audit multi-plateformes** — visualisez les modifications sur les serveurs de fichiers Windows, les clusters à basculement, les baies NetApp, les NAS Synology et Hitachi, EMC VNX, VNXe, Isilon, Celerra et Unity, depuis une console unique.

## Audit des paramètres de stratégie de groupe

CONTRÔLEURS DE DOMAINE

- **Auditez les objets de stratégie de groupe** — surveillez la création, la suppression et la modification des objets GPO.
- **Suivez les modifications des paramètres GPO** — identifiez qui a modifié quel paramètre, à quel moment, depuis quel emplacement, et comparez les valeurs avant et après.
- **Consultez l'historique des modifications** — visualisez l'historique d'un ou plusieurs GPO dans un domaine afin de détecter toute activité suspecte ou non autorisée.
- **Configurez des alertes sur les changements critiques** — alertes instantanées par e-mail et SMS, par exemple sur la configuration des ordinateurs ou les stratégies de verrouillage de compte et de mot de passe.
- **Planifiez l'envoi de rapports** — envoi automatique de rapports sur les modifications importantes des GPO ou de leurs paramètres, à des destinataires définis.

## Audit et rapports sur les serveurs Windows

SERVEURS WINDOWS

- **Auditez les serveurs Windows** — modifications des appartenances aux groupes administratifs locaux, des utilisateurs locaux, des droits des utilisateurs et des stratégies locales.
- **Suivez les tâches planifiées et les processus** — rapports sur leur création, leur suppression et leur modification.
- **Surveillez les périphériques USB et les imprimantes** — utilisation des ports USB et transferts vers des supports externes ; documents imprimés avec nom du fichier, date et heure, utilisateur, nombre de pages et de copies.
- **Auditez les processus PowerShell** — processus exécutés sur vos serveurs Windows et commandes lancées.
- **Surveillez ADFS, LAPS et ADLDS** — tentatives d'authentification via ADFS, utilisateurs ayant consulté les mots de passe administrateur locaux, modifications des dates d'expiration des mots de passe.

# Les accès, les comptes et les menaces

## Audit des connexions et déconnexions

CONTRÔLEURS DE DOMAINE · SERVEURS WINDOWS · POSTES DE TRAVAIL

- **Auditez les connexions et déconnexions** — activité et durée des sessions sur vos contrôleurs de domaine, serveurs et postes.
- **Suivez l'historique de connexion** — identifiez les utilisateurs connectés et ceux qui le sont sur plusieurs machines.
- **Auditez les connexions RADIUS** — rapports sur les connexions réussies, les échecs et l'historique des connexions RADIUS (NPS).
- **Analysez les échecs de connexion** — toutes les tentatives échouées, avec l'utilisateur, la machine ciblée, l'heure et la raison de l'échec.
- **Réagissez aux connexions malveillantes** — l'IA détecte les volumes inhabituels d'échecs et les horaires suspects.

## Analyse des verrouillages de comptes

CONTRÔLEURS DE DOMAINE · SERVEURS WINDOWS · POSTES DE TRAVAIL

- **Recevez des notifications de verrouillage** — détection en temps réel des verrouillages de comptes AD par e-mail et SMS, pour en réduire la durée.
- **Identifiez la source** — connexions mobiles, sessions RDP, services, tâches planifiées : repérez les identifiants obsolètes.
- **Vérifiez l'état de chaque compte** — rapports détaillant l'état de chaque compte verrouillé et l'heure du verrouillage.
- **Analysez les verrouillages par l'UBA** — repérez les utilisateurs négligents et les menaces internes via les verrouillages anormaux.
- **Améliorez l'efficacité du support** — le service desk a tout pour résoudre vite et limiter les interruptions.
- **Analysez la cause racine** — piste d'audit claire des réinitialisations, modifications et sources de verrouillage, exploitable en forensique.

## Surveillance de l'activité des employés

POSTES DE TRAVAIL

- **Mesurez la productivité** — heures de démarrage et d'arrêt, historique des connexions, activités sur les fichiers.
- **Suivez l'assiduité** — feuilles de temps précises avec heures d'arrivée et de départ, et analyse de la durée des connexions.
- **Calculez les heures réelles** — utilisateurs connectés et temps de travail effectif, périodes d'inactivité incluses.
- **Surveillez le travail à distance** — connexions via passerelle RDG et RADIUS : qui, quand, avec quel résultat et pour quelle durée.
- **Surveillez l'activité des postes** — derniers horaires de démarrage et d'arrêt, utilisateur à l'origine, type d'arrêt.
- **Identifiez les connexions à risque** — tentatives échouées répétées sur les postes, machines distantes ou serveurs critiques.

## Surveillance des utilisateurs à privilèges

CONTRÔLEURS DE DOMAINE · SERVEURS WINDOWS

- **Auditez l'activité des administrateurs** — actions sur le schéma AD, la configuration, les utilisateurs, groupes, OU et GPO.
- **Examinez les activités à privilèges** — piste d'audit complète des actions réalisées par les utilisateurs à privilèges dans votre domaine.
- **Détectez les élévations de privilèges** — première utilisation d'un privilège par un utilisateur, à confronter à son rôle.
- **Repérez les anomalies comportementales** — actions inhabituelles au regard des accès normaux, pour identifier les identifiants volés.
- **Recevez des alertes sur les activités suspectes** — suppression des journaux d'audit, accès à des données sensibles en dehors des heures ouvrables.

## Détection des malwares et des menaces internes

TOUS LES MODULES

- **Chasse aux menaces via l'UBA** — échecs de connexion répétés, anomalies d'activité utilisateur, élévations de privilèges, exfiltrations de données.
- **Détectez les rançongiciels** — pics inhabituels de renommage, suppression ou modification des autorisations de fichiers.
- **Réagissez instantanément** — scripts automatiques pour éteindre des machines ou mettre fin à des sessions.
- **Identifiez les anomalies sur les fichiers** — suppression de fichiers critiques, pics d'accès, activités à des heures inhabituelles.
- **Détectez les mouvements latéraux** — activités inhabituelles via le bureau à distance ou exécution de nouveaux processus sur le réseau.

## Rapports de conformité

TOUS LES MODULES

- **Exploitez plus de 250 rapports** — changements dans Active Directory, sur les serveurs de fichiers, les serveurs Windows et les postes.
- **Recevez des rapports prêts à l'emploi** — envoi périodique pour HIPAA, PCI DSS, RGPD, ISO 27001, GLBA, FISMA et SOX, personnalisables.
- **Réalisez des analyses de causes profondes** — identifiez la source des fuites ou intrusions et partagez vos conclusions.
- **Surveillez l'intégrité des fichiers** — accès aux fichiers système, bases de données, logiciels et archives d'audit.
- **Configurez des alertes instantanées** — par e-mail et SMS, ciblées sur des fichiers, utilisateurs ou plages horaires ; l'UBA réduit les faux positifs.
- **Limitez les dégâts** — scripts automatisés pour désactiver des comptes ou éteindre des appareils.

# Trois éditions. On vous aide à choisir la vôtre.

ÉDITION GRATUITE

## Jamais expirée

- Audit et collecte de données sur 25 postes de travail
- Génération de rapports à partir des données de journaux collectées pendant l'évaluation

ÉDITION STANDARD

## À partir de 595 €/an

- Toutes les fonctions de l'édition gratuite
- Rapports et alertes sur les journaux d'événements collectés depuis les composants sous licence : contrôleurs de domaine, tenants Azure AD, serveurs Windows, postes de travail, serveurs de fichiers Windows et périphériques NAS

ÉDITION PROFESSIONNELLE

## À partir de 945 €/an

- Toutes les fonctions de l'édition Standard
- Analyse des verrouillages de comptes
- Audit des modifications des permissions AD
- Audit des modifications des paramètres GPO
- Audit des modifications DNS et du schéma AD
- Valeurs anciennes et nouvelles des attributs des objets AD
- Prise en charge des bases de données MS SQL

| MODULE DE LICENCE | ABONNEMENT ANNUEL |
|---|---|
| **Contrôleurs de domaine**<br>module principal — 2 contrôleurs, édition Standard | à partir de 595 € |
| **MODULES COMPLÉMENTAIRES** | |
| **Tenants Azure AD**<br>1 tenant | à partir de 995 € |
| **Serveurs de fichiers Windows**<br>2 serveurs | à partir de 495 € |
| **Serveurs NAS**<br>EMC, NetApp, Synology, Hitachi, Huawei… — 1 serveur | à partir de 595 € |
| **Serveurs Windows**<br>5 serveurs | à partir de 345 € |
| **Postes de travail**<br>100 postes | à partir de 245 € |
| **Sauvegarde et récupération AD**<br>250 objets utilisateur AD activés | à partir de 195 € |

Tarifs publics éditeur, abonnement annuel — source : ManageEngine, page de tarification ADAudit Plus (manageengine.com/products/active-directory-audit/pricing-details.html), consultée le 13/08/2026. La licence est **modulaire et par serveur** : chaque périmètre audité se souscrit séparément, et les montants ci-dessus correspondent au premier palier de chaque module, indiqué sous son intitulé. Prix indicatifs et non contractuels : le montant applicable dépend de l'édition, du nombre de contrôleurs de domaine, de serveurs, de postes et des modules retenus. L'éditeur propose des paliers intermédiaires sur devis. Devis personnalisé LAZAR SOFT sur demande.

# Contactez-nous.

Une question ou un chiffrage précis : un #RocketExpert vous répond sous 24 h ouvrées.

TÉLÉPHONE
+33 (0)1 76 21 60 43

E-MAIL
sales@lazarsoft.com