ManageEngine
Log360

Les composants d'une licence Log360

Expliqués

https://www.manageengine.com/fr/log-management/

Composant	Quand vous en avez besoin	Ce que vous devez faire	Critères de tarification
Sources de journaux	Pour collecter les journaux depuis : appareils Syslog, serveurs Windows, sites IIS, serveurs MSSQL, serveurs de fichiers Linux, autres applications et machines virtuelles.	Précisez le nombre de sources de logs sur votre réseau. Si le système d'exploitation et les applications d'une machine sont surveillés, une seule licence de source de logs est nécessaire pour ce système.	Sur la base du nombre d'appareils ajoutés comme sources de logs, avec un minimum de 10 sources requises.
Terminaux	Pour l'audit de vos terminaux Windows et Mac.	Spécifiez le nombre de terminaux à auditer.	Disponible par pack de 100. Le pack de base comprend 100 postes de travail.
Comptes cloud	Pour superviser et auditer les événements des sources cloud, tels que les locataires Office 365 et les comptes AWS.	Précisez le nombre de locataires Office 365 et de comptes AWS.	Aucun pack de base ou minimum n'est requis pour les locataires cloud.
Contrôleurs de domaine	Pour auditer les activités de votre Active Directory.	Indiquez le nombre de contrôleurs de domaine à auditer.	Facturation basée sur le nombre de contrôleurs de domaine ajoutés, avec un minimum de 2.
Serveurs de fichiers	Pour auditer les serveurs de fichiers, notamment : Windows File Servers, NetApp, EMC, Huawei, CTERA, Synology, QNAP, Nutanix, Azure File Share et Amazon FSx.	Précisez le nombre de serveurs de fichiers à auditer.	Aucun pack de base ou quantité minimale n'est requis pour les serveurs de fichiers.

Modules complémentaires

Composant	Quand vous en avez besoin	Ce que vous devez faire	Critères de tarification
Sauvegarde et restauration AD	Pour sauvegarder et restaurer les objets, attributs et configurations de domaine Active Directory.	Activer le module complémentaire	Basé sur le nombre de contrôleurs de domaine achetés

Nos produits

AD360 | ADAudit Plus | EventLog Analyzer | DataSecurity Plus | Exchange Reporter Plus | M365 Manager Plus

À propos de Log360

Log360 est une solution SIEM unifiée avec des capacités DLP et CASB intégrées qui détecte, priorise, examine et répond aux menaces de sécurité. Vigil IQ, le module TDIR de la solution, combine des informations sur les menaces, un atelier d'analyse des incidents, une détection des anomalies basée sur le ML et des techniques de détection des attaques basées sur des règles pour détecter les attaques sophistiquées.
Il offre également une console de gestion des incidents pour remédier efficacement aux menaces détectées. Log360 offre une visibilité holistique de la sécurité sur les réseaux sur site, cloud et hybrides grâce à ses capacités intuitives et avancées d'analyse et de surveillance de la sécurité.

Pour plus d'informations sur Log360, visitez le site https://www.manageengine.com/fr/log-management/ et suivez la page LinkedIn pour obtenir des mises à jour régulières .

$ Obtenir un devis

Télécharger