AYI NEDJIMI Consultants

Graylog : Plateforme SIEM Log Management Open Core

10 mai 2026 • Mis à jour le 17 mai 2026 • 18 min de lecture •

3630 mots • 67 vues •

Graylog est une plateforme SIEM (Security Information and Event Management) et de log management centralise distribuee selon un modele open core par la societe Graylog Inc. (Houston, Texas, anciennement Hambourg). Concue pour ingerer, indexer, correler et analyser plusieurs teraoctets de logs par jour avec une latence inferieure a la seconde, la plateforme combine un coeur open source Graylog Open sous licence SSPLv1 et des editions commerciales Graylog Operations, Graylog Security et Graylog Enterprise. Demarree en 2010 a Hambourg par Lennart Koopmann sous le nom Graylog2, la solution atteint la version 6.2 en mai 2026 et compte plus de 50 000 deploiements declares dont environ 1 800 clients commerciaux. Graylog repose sur une architecture trois

> tiers : un cluster Graylog Server (JVM Java 17), une base MongoDB et un backend Elasticsearch ou OpenSearch.

Graylog est une plateforme **SIEM (Security Information and Event Management)** et de **log management centralise** distribuee selon un modele **open core** par la societe **Graylog, Inc.** (Houston, Texas, anciennement Hambourg). Concue pour ingerer, indexer, correler et analyser plusieurs teraoctets de logs par jour avec une latence inferieure a la seconde, la plateforme combine un coeur open source **Graylog Open** sous licence **SSPLv1** et des editions commerciales **Graylog Operations**, **Graylog Security** et **Graylog Enterprise**. Demarree en 2010 a Hambourg par **Lennart Koopmann** sous le nom Graylog2, la solution atteint la **version 6.2** en mai 2026 et compte plus de **50 000 deploiements** declares dont environ 1 800 clients commerciaux. Graylog repose sur une architecture trois tiers : un cluster **Graylog Server** (JVM Java 17, traitement des messages), une base **MongoDB** (configuration, utilisateurs, dashboards) et un backend de recherche **Elasticsearch ou OpenSearch** (stockage des messages et index inverse). Cette dissociation entre stockage, configuration et processing donne a Graylog une scalabilite horizontale lineaire et un avantage de cout face a Splunk Enterprise ou IBM QRadar.

Réponse sous 24h

Devis gratuit →