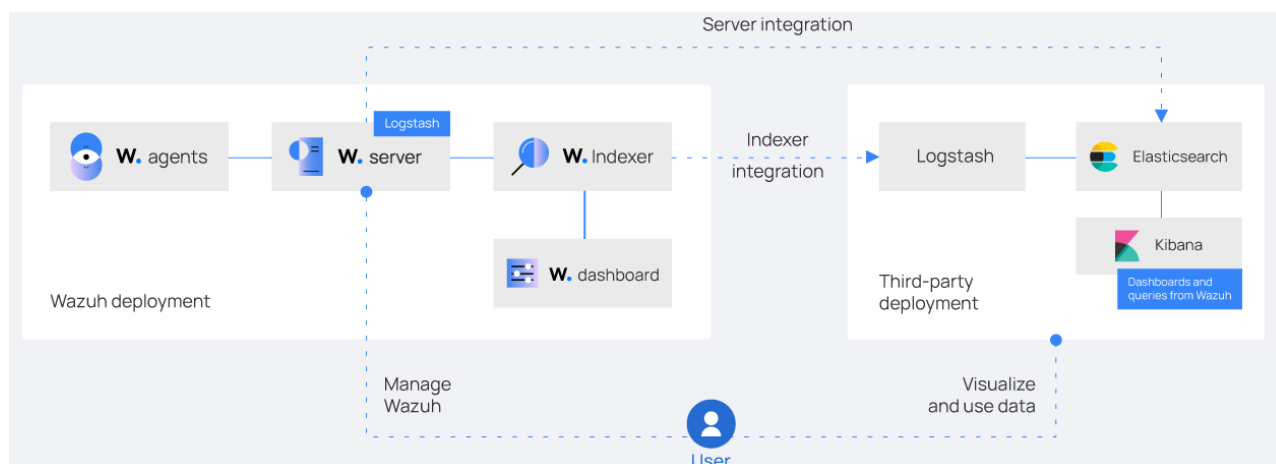


FICHE 1 – SIEM WAZUH – ARCHITECTURE

Lien officiel de l'installation :

<https://documentation.wazuh.com/current/installation-guide/index.html>

Wazuh est une plateforme de sécurité qui fournit une protection XDR et SIEM unifiée pour les points d'extrémité et les charges de travail en nuage. La solution est composée d'un seul agent universel et de trois composants centraux : le **serveur Wazuh**, l'**indexeur Wazuh** et le **tableau de bord Wazuh**.



Wazuh est libre et open source. Ses composants se conforment à la Licence Publique Générale GNU, version 2, et à la Licence Apache, Version 2.0 (ALv2).

L'indexeur Wazuh et le serveur Wazuh peuvent être installés sur un seul hôte ou sur des hôtes séparés.

A. L'INDEXEUR WAZUH

L'indexeur Wazuh est un moteur de recherche et d'analyse en texte intégral très évolutif. Ce composant central de Wazuh indexe et stocke des alertes générées par le serveur Wazuh et fournit des capacités de recherche et d'analyse de données en temps quasi réel.

Vous pouvez installer l'indexeur Wazuh sur un seul hôte. Alternativement, vous pouvez l'installer distribué dans plusieurs nœuds, dans une configuration de cluster. Cela permet d'améliorer la haute disponibilité et les performances.

B. LE SERVEUR WAZUH

Le serveur Wazuh analyse les données reçues des agents Wazuh, déclenchant des alertes lorsque des menaces ou des anomalies sont détectées. Il est également utilisé pour gérer à distance la configuration des agents et surveiller leur statut.

Vous pouvez installer le serveur Wazuh sur un seul hôte ou vous pouvez l'installer distribué en plusieurs nœuds dans une configuration de cluster. Les configurations multi-nœuds offrent une disponibilité élevée et des performances améliorées. Et s'il est combiné à un équilibreur de charge de réseau, une utilisation efficace de sa capacité peut être réalisée.

Le serveur Wazuh comprend deux composants principaux: le gestionnaire de Wazuh et le fichier. Le gestionnaire de Wazuh est responsable de l'analyse et de l'alerte des données, tandis que l'intégration de l'indexeur transmet les données analysées à l'indexateur Wazuh.

C. TABLEAU DE BORD DE WAZUH

Cette composante centrale est une interface Web flexible et intuitive pour l'extraction, l'analyse et la visualisation des données de sécurité. Il fournit des tableaux de bord prêts, vous permettant de naviguer de manière transparente à travers l'interface utilisateur.

Avec le tableau de bord Wazuh, les utilisateurs peuvent visualiser les événements de sécurité, les vulnérabilités détectées, les données de surveillance de l'intégrité des fichiers, les résultats d'évaluation de la configuration et les normes de conformité à la réglementation.

D. AGENT WAZUH

L'agent Wazuh est multi-plateforme et fonctionne sur les points d'extrémité que l'utilisateur souhaite surveiller. Il communique avec le serveur Wazuh, envoyant des données en temps quasi réel via un canal crypté et authentifié.

L'agent a été développé en tenant compte de la nécessité de surveiller une grande variété de différents critères d'évaluation sans avoir d'impact sur leurs performances. Il est supporté par les systèmes d'exploitation les plus populaires, et il nécessite 35 Mo de RAM en moyenne.

L'agent Wazuh fournit des fonctionnalités clés pour améliorer la sécurité de votre système.

- Collecteur de logs
- Exécution du commandement
- Surveillance de l'intégrité des fichiers (FIM *File integrity monitoring*)
- Évaluation de la configuration de sécurité (SCA *Security configuration assessment*)
- Inventaire du système
- Détection de logiciels malveillants
- Réponse active



La compatibilité entre l'agent Wazuh et le gestionnaire Wazuh est garantie lorsque la version du gestionnaire de Wazuh est postérieure ou égale à celle de l'agent Wazuh.

Vous pouvez également déployer un nouvel agent en suivant les instructions du tableau de bord de Wazuh. Allez dans Endpoints Summary, et cliquez sur Déployer un nouvel agent.