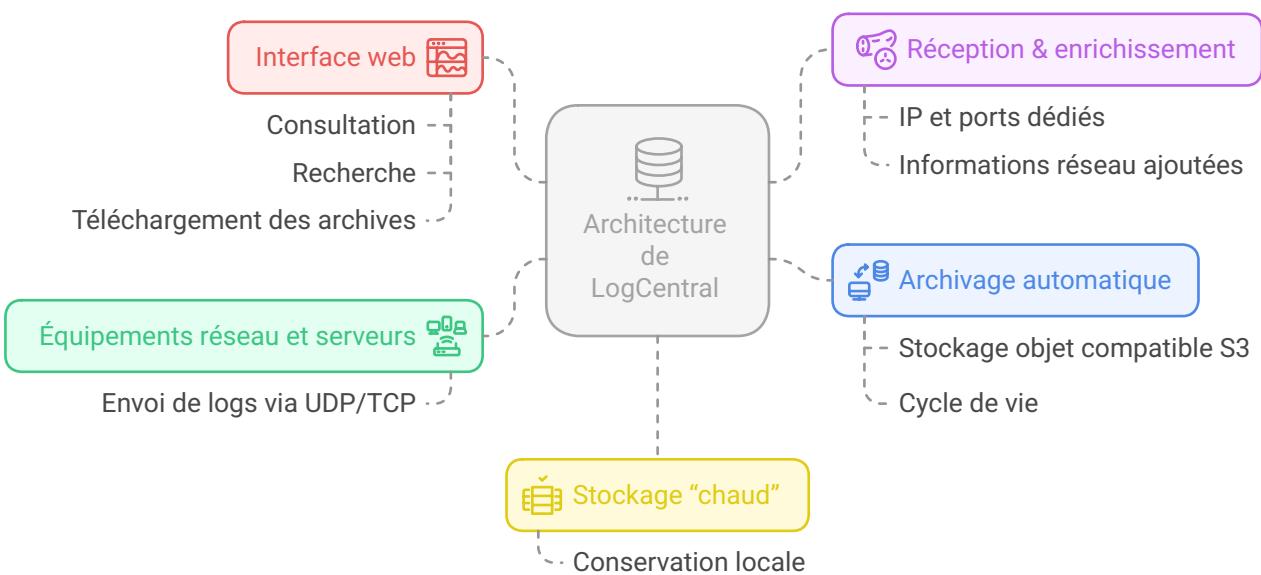


PAPIER BLANC

[+] LOGCENTRAL

La centralisation des logs pour une supervision réseau proactive

Architecture de LogCentral



Résumé exécutif

La dispersion des journaux systèmes (syslogs) sur plusieurs sites et équipements rend la consultation et l'analyse chronophages. Les équipes IT doivent jongler entre différentes interfaces et emplacements pour accéder à l'information.

La **centralisation des logs dans une plateforme unique** comme **LogCentral** simplifie cette tâche : tous les journaux sont collectés au même endroit, enrichis d'informations contextuelles, et accessibles via une interface web. Ce document présente les bénéfices, l'architecture et des exemples concrets d'usages.

La centralisation des logs pour une supervision réseau proactive

Contexte & enjeux

- Les infrastructures réseau actuelles sont géographiquement distribuées.
- Les équipements (switches, firewalls, serveurs, IoT...) génèrent des logs critiques pour le diagnostic.
- Le stockage local rend difficile :
 - La consultation rapide lors d'un incident.
 - L'accès aux logs d'un site distant.
 - La conservation fiable à long terme.

Problématique

Comment garantir un accès rapide et fiable aux logs provenant de multiples sites, tout en assurant un stockage conforme et centralisé ?

Sans centralisation :

- Nécessité de se connecter à chaque équipement ou serveur pour consulter les logs.
- Risque de perte de données en cas de panne locale.
- Pas de vue consolidée de l'activité réseau.

Solution : la centralisation avec LogCentral

LogCentral permet de :

- Recevoir les logs de tous vos sites via des IP/ports dédiés.
- Enrichir les données (fournisseur d'accès, pays, ville quand disponible).
- Accéder aux journaux via une interface web centralisée.
- Archiver automatiquement les logs sur un stockage objet en Europe avec politiques de rétention.
- Ne pas vous préoccuper de l'infrastructure de syslog

Bénéfices :

- Gain de temps dans l'accès aux données.
- Réduction des risques de perte grâce à l'archivage centralisé.
- Historisation fiable pour audits ou analyses ultérieures.
- Simplicité d'accès pour les équipes réparties sur plusieurs sites.

La centralisation des logs pour une supervision réseau proactive

Architecture type avec LogCentral

- Équipements réseau et serveurs → envoi de logs via UDP/TCP vers l'adresse LogCentral.
- Réception & enrichissement → IP et ports dédiés par site, informations réseau ajoutées.
- Stockage "chaud" → conservation locale pour accès rapide.
- Archivage automatique → stockage objet compatible S3 en Europe, cycle de vie
- Interface web → consultation, recherche et téléchargement des archives.

Cas d'usage concret

Entreprise multi-sites (exemple réel de configuration)

- **Avant :** les équipes IT devaient se connecter à chaque firewall pour récupérer les logs lors d'un incident.
- **Après :** avec LogCentral, tous les journaux sont disponibles depuis une interface unique, même pour des événements ayant eu lieu plusieurs mois auparavant, sans devoir interroger chaque équipement.

Conclusion

La centralisation des logs offre un accès rapide, sécurisé et structuré à des données essentielles. Avec LogCentral, vous disposez d'une solution clé en main pour regrouper et conserver vos syslogs, tout en respectant les exigences de conformité européennes.

→ Contactez-nous pour découvrir comment LogCentral peut simplifier la gestion et l'accès à vos logs, quelle que soit la taille de votre réseau.