

## Formation Graylog

<b>Durée :</b>	3 jours
<b>Public :</b>	Administrateurs système
<b>Pré-requis :</b>	Pratique de base de l'administration d'un système Linux
<b>Objectifs :</b>	Découverte et prise en main de la solution Graylog de centralisation et supervision de logs
<b>Sanction :</b>	Attestation de fin de stage mentionnant le résultat des acquis
<b>Taux de retour à l'emploi:</b>	Aucune donnée disponible
<b>Référence:</b>	RéS101324-F
<b>Note de satisfaction des participants:</b>	4,91 / 5

### Découvrir Graylog

Intérêt de la centralisation

- Sécurisation
- Exploitation
- Monitoring

Solutions centralisées  
Graylog vs ELK

### Installer et configurer Graylog

Fonctionnalités  
Architecture  
Installation  
Configuration initiale

#### **Atelier : Installation de l'écosystème graylog**

### Prendre en main la solution Graylog

Comprendre la journalisation

- Les types de journalisation
- Linux
- Windows
- Équipements réseaux
- Micro-services Docker

Créer un canal d'entrée  
Test d'envoi de log  
Visualisation des logs reçus

#### **Atelier : Centralisation des logs d'un système Linux et d'un conteneur Docker**

## **Rediriger les messages - Streams**

Notion de streams  
Streams vs Recherches  
Création de stream  
Index associés

**Atelier : Création d'une catégorie pour les micro-services et d'une catégorie pour les échecs de connexion SSH**

## **Paramétrer la rétention**

Intérêt de la rétention  
Stratégies de rétention  
Configuration de la rétention

**Atelier : Création de rétention pour les catégories créées**

## **Comprendre les recherches Graylog**

Fenêtre temporelle  
Critères de recherche  
Gestion des champs  
Sauvegarde d'une recherche  
Exportation du résultat d'une recherche  
Ajout d'un widget à une recherche

**Atelier : Création et sauvegarde d'une recherche avancée**

## **Gérer les dashboards**

Dashboard et recherche  
Création d'un dashboard  
Utilisation d'un dashboard  
Ajout d'une recherche à un dashboard

**Atelier : Création d'un dashboard et intégration d'une recherche**

## **Gérer les évènements et alertes**

Présentation  
Création d'évènement  
Affichage des évènements  
Création d'une notification

**Atelier : Mise en place d'une alerte**