DAWAN

Plan de la formation

www.dawan.fr

Formation Graylog

Durée :	3 jours (21 heures)
Tarifs inter-entreprise :	2 475,00 € HT (standard) 1 980,00 € HT (remisé)
Public :	Administrateurs système
Pré-requis :	Pratique de base de l'administration d'un système Linux
Objectifs :	Découverte et prise en main de la solution Graylog de centralisation et supervision de logs
Modalités pédagogiques, techniques et d'encadrement :	• Formation synchrone en présentiel et distanciel. • Méthodologie basée sur l'Active Learning : 75 % de pratique minimum. • Un PC par participant en présentiel, possibilité de mettre à disposition en bureau à distance un PC et l'environnement adéquat. • Un formateur expert.
Modalités d'évaluation :	• Définition des besoins et attentes des apprenants en amont de la formation. • Auto-positionnement à l'entrée et la sortie de la formation. • Suivi continu par les formateurs durant les ateliers pratiques. • Évaluation à chaud de l'adéquation au besoin professionnel des apprenants le dernier jour de formation.
Sanction :	Attestation de fin de formation mentionnant le résultat des acquis
Référence :	RéS101324-F
Note de satisfaction des participants:	4,91 / 5
Contacts :	commercial@dawan.fr - 09 72 37 73 73
Modalités d'accès :	Possibilité de faire un devis en ligne (www.dawan.fr, moncompteformation.gouv.fr, maformation.fr, etc.) ou en appelant au standard.

Délais d'accès :	Variable selon le type de financement.
Accessibilité :	Si vous êtes en situation de handicap, nous sommes en mesure de vous accueillir, n'hésitez pas à nous contacter à referenthandicap@dawan.fr, nous étudierons ensemble vos besoins

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 containeur 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