DAWAN

Plan de la formation

www.dawan.fr

Formation Elastic pour DevOps : logs centralisés en environnement Kubernetes & cloud

Durée :	2 jours (14 heures)
Tarif inter-entreprise :	1 875,00 € HT (standard) 1 500,00 € HT (remisé)
Public :	Ingénieurs DevOps - Administrateurs systèmes et réseaux - Ingénieurs cloud - Exploitants - SRE - Toute personne souhaitant centraliser et exploiter des logs dans un environnement conteneurisé ou cloud
Pré-requis :	Avoir suivi la formation Elastic : Initiation ou disposer de connaissances équivalentes - Connaître les bases d'Elasticsearch et de Kibana - Disposer de connaissances générales en administration Linux, conteneurisation ou exploitation de services - Une première expérience de Docker, Kubernetes ou du cloud est recommandée
Objectifs :	Comprendre l'usage d'Elastic dans une démarche DevOps et d'exploitation moderne - Collecter et centraliser des logs issus d'environnements Linux, Docker, Kubernetes et cloud - Exploiter les logs pour diagnostiquer des incidents applicatifs et d'infrastructure - Construire des tableaux de bord utiles aux équipes DevOps - Mettre en place des alertes simples et appliquer les bonnes pratiques d'exploitation
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.

Modalité 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 :	RéS102933-F
Note de satisfaction des participants :	4,66 / 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

Comprendre l’apport d’Elastic dans une démarche DevOps

Positionner Elastic dans une chaîne DevOps et d’exploitation moderne
Identifier les cas d’usage de centralisation des logs dans des environnements conteneurisés et cloud
Relier collecte, recherche, analyse et visualisation dans une logique de diagnostic et d’amélioration continue
Différencier Elastic des autres outils de monitoring et d’observabilité fréquemment utilisés
Atelier pratique : Explorer une architecture DevOps intégrant Elastic pour la centralisation et l’analyse des logs

Collecter les logs d’environnements Linux, conteneurisés et cloud

Identifier les sources de logs issues des systèmes, des conteneurs, des orchestrateurs et des services cloud
Comprendre les principes de collecte adaptés aux environnements modernes
Préparer l’intégration de logs applicatifs, systèmes et techniques dans Elastic

Structurer les flux pour faciliter l’analyse et l’exploitation
Atelier pratique : Mettre en place une collecte de logs provenant de plusieurs sources techniques

Intégrer Elastic dans un environnement Docker et Kubernetes

Comprendre les spécificités de la journalisation dans les environnements conteneurisés
Identifier les points de vigilance liés aux pods, aux nœuds et aux services
Centraliser les logs produits par des conteneurs et des applications déployées sur Kubernetes
Préparer une exploitation cohérente des données dans un contexte dynamique et distribué
Atelier pratique : Centraliser et consulter des logs issus d’un environnement Docker ou Kubernetes

Exploiter les logs pour diagnostiquer les incidents

Rechercher rapidement des événements pertinents dans des volumes importants de logs
Filtrer, corréler et contextualiser les informations utiles
Identifier des erreurs applicatives, des anomalies système et des incidents de déploiement
Utiliser Elastic pour accélérer l’analyse et la résolution de problèmes
Atelier pratique : Diagnostiquer un incident applicatif ou d’infrastructure à partir des logs centralisés

Construire des tableaux de bord utiles aux équipes DevOps

Définir les indicateurs pertinents pour le suivi d’une plateforme ou d’une application
Concevoir des visualisations orientées exploitation, diagnostic et suivi de déploiement
Organiser des tableaux de bord lisibles pour les équipes techniques
Faciliter l’analyse des incidents, des erreurs récurrentes et des tendances d’exploitation
Atelier pratique : Réaliser un tableau de bord Kibana orienté exploitation DevOps

Mettre en place des alertes et fiabiliser l’exploitation

Identifier les événements devant déclencher une alerte
Définir des règles de détection utiles et exploitables

Réduire le bruit en ciblant les signaux réellement significatifs
Préparer une démarche d’exploitation plus proactive dans des environnements en évolution rapide
Atelier pratique : Configurer des alertes simples et exploiter les remontées pour améliorer la supervision

Appliquer Elastic à des scénarios cloud et de production

Relier Elastic aux besoins de suivi d’applications déployées sur le cloud
Prendre en compte les contraintes de volumétrie, de rotation et de conservation des logs
Identifier les bonnes pratiques pour exploiter Elastic dans un contexte de production
Préparer l’évolution vers des usages plus avancés d’observabilité et de troubleshooting
Atelier pratique : Étudier un cas complet de centralisation, d’analyse et de suivi des logs en environnement cloud