

Formation Administrer Elasticsearch

Présentation

Cette formation couvre l'installation et l'estimation des ressources nécessaires pour une infrastructure, incluant l'allocation des shards, le déploiement, et le paramétrage des ressources. Elle aborde également la surveillance, la maintenance, et la sécurité des clusters, ainsi que l'optimisation des performances et la réplication entre clusters.

Durée : 14,00 heures (2 jours)

Tarif INTRA : Nous consulter

Objectifs de la formation

- Apprendre à mettre en place la stack ELK
- Dimensionner les éléments matériels
- Surveiller Elasticsearch
- Administrer la plateforme dans différentes configurations

Prérequis

- Connaissance des fondamentaux du système d'exploitation Linux
- Ligne de commande et commandes de base
- Une connexion internet, idéalement accès SSH sur internet est nécessaire.

Public

- Administrateurs système et réseaux, SRE, devops, développeurs ...

Programme de la formation

Installer & estimer les ressources nécessaires d'infrastructure

- Allocation des *shards*, commandes et philosophie :
 - Déploiement classique



- Déploiement multi *data tiers*
- Rôles des nœuds
- Savoir expliquer les allocations effectuées
- *Recovery*: Quand et comment les contrôler
- Explications du *routing* des requêtes de recherche et d'indexation
- Nœuds *master* et *voting* configuration
- Paramétrage de la mémoire
- Paramétrage du disque
- Paramétrage réseau
- Paramétrage CPU
- Avertissement sur la virtualisation
- Recette de dimensionnement
- Usage API pour lister les fonctionnalités X-Pack actives

Monitorer & réagir

- API Cluster *Health*, Cluster stats/state, Node infos/stats, Index _stats
- APIs équivalentes avec l'API _cat
- Connaître les tâches en attente de traitement sur le cluster (*pending tasks*)
- Connaître les threads les plus actifs d'un nœud (*hot threads*)
- Monitorer les fonctionnalités du *stack*
- Monitorer la mémoire utilisée
- Monitorer les file *handles* utilisés
- Monitorer l'occupation disque
- Monitorer la bande passante et connexions réseau
- Surveiller les indicateurs de performance : charge de travail des *threads*, performances d'indexation/recherche et surveillance des requêtes "lentes"
- Monitorer à l'aide des journaux applicatifs Elasticsearch
- Alerter sur la base des données de monitoring

Maintenance

- Mécanismes du *Recovery*
- Se mettre à l'échelle : ajouter ou retirer un nœud
- Opérations de maintenance : redémarrer un nœud ou un *cluster* complet
- Ré-indexer des données
- Prévenir les arrêts de services : *Aliases* et *Rollover* API

- Cas particulier d'usage des indices : les *DataStream*s
- Sauvegarder et restaurer des indices
- Fonctionnalité de sauvegarde automatisée (*Snapshot Lifecycle Management* ou SLM)
- Fonctionnalité de gestion du cycle de vie des indices (*Index Lifecycle Management* ou ILM)
- Utiliser l'API de dépréciation
- Préparer une montée de version
- Monter de version

Sécurité

- Périmètre et vue d'ensemble
- Filtrer les flux réseau
- Limiter les fonctionnalités de *scripting*
- Chiffrer les données sur disque ou échangées sur le réseau
- Authentifier les utilisateurs avec X-Pack *security*
- Authentifier les utilisateurs avec un *reverse proxy*
- Autorisations d'accès aux ressources

Cross Cluster Replication (CCR)

- Répliquions entre clusters distants unidirectionnelles ou bidirectionnelles pour permettre différents cas d'usage :
 - Une architecture capable un retour rapide à la normale après désastre
 - Une architecture de mise à proximité données
 - Une architecture de centralisation de la supervision

Optimisation & Performance

- Indexer plus rapidement :
 - Bulk API
 - *Refresh interval*
 - Optimisations des *mappings*
- Rechercher plus efficacement :
 - Contextes de filtres, de post *filters*, opérateurs "exact matches" et caches
 - Pièges des opérateurs *wildcard* ou des *mappings parent/child*

- Agréger and trier plus efficacement : *doc_values* et *fielddata*
- Diagnostiquer le calcul de score, ou les erreurs
- Profiler ses recherches pour comprendre les temps de réponse
- Matériel & Infrastructure :
 - Penser aux capacités de gestion des *data tiers* d'Elasticsearch
 - Pas d'ingestion sans nœud dédié à cette activité
 - Dissocier les clusters pour les spécialiser dans des tâches données (supervision vs métier)

Organisation

Formateur

Les formateurs de Docaposte Institute sont des experts de leur domaine, disposant d'une expérience terrain qu'ils enrichissent continuellement. Leurs connaissances techniques et pédagogiques sont rigoureusement validées en amont par nos référents internes.

Riches de leur expérience sur le sujet, ils sauront accompagner vos collaborateurs dans leur montée en compétence.

Moyens pédagogiques et techniques

- Alternance d'apports théoriques et de mises en pratique contextualisées.
- Progression pédagogique structurée, de la compréhension à la mise en œuvre opérationnelle.
- Pédagogie immersive favorisant une mise en application immédiate des compétences.
- Formation interactive et participative s'appuyant sur des ateliers pratiques, études de cas et échanges collectifs (+ 60 % du temps de formation.)
- Séquences pédagogiques rythmées et évaluations formatives régulières pour renforcer l'ancrage des apprentissages.
- Supports de cours, ressources documentaires et références mis à disposition par le formateur

Dispositif de suivi de l'exécution et de l'évaluation des résultats de la formation

En amont de la formation (*évaluation en ligne dans l'extranet apprenant*)

- Recueil des besoins et des attentes des participants.
- Auto-positionnement permettant d'évaluer le niveau initial des apprenants.

Tout au long de la formation

- Évaluations continues réalisées par le formateur à travers des questions orales, exercices, QCM, études de cas et mises en situation pratiques.

À l'issue de la formation (*évaluations en ligne dans l'extranet apprenant*)

- Auto-positionnement afin de mesurer l'acquisition des compétences visées.
- Validation de l'acquisition des compétences par le formateur
- Questionnaire de satisfaction « à chaud » à l'issue de la formation
- Questionnaire de satisfaction "à froid", 45 jours après la formation afin d'évaluer l'ancrage des acquis et leur mise en application en situation professionnelle.

Accessibilité

Nos formations peuvent être adaptées à certaines conditions de handicap. Nous contacter pour toute information et demande spécifique.