alter way

Formation officielle Docker (Bundle) :

Mirantis Kubernetes Engine (MKE) + Mirantis Secure Registry (MSR)

Durée 2 jours (14h)

Dans ce cours axé sur le produit, vous plongerez dans toutes les fonctionnalités de Mirantis Kubernetes Engine et découvrirez comment il simplifie, sécurise et accélère la gestion des clusters Kubernetes et Swarm à l'échelle de l'entreprise. Nous aborderons l'installation et la configuration de MKE, la gestion des permissions des utilisateurs MKE et des ressources de l'orchestrateur, les fonctions avancées de mise en réseau incluses dans la plateforme, ainsi que le dépannage et le support de MKE.

Vous plongerez également dans toutes les fonctionnalités de Mirantis Secure Registry et découvrirez comment il peut améliorer la sécurité de la production, du stockage et de la distribution de vos images de conteneurs, en tant que registre autonome ou intégré dans un pipeline d'intégration continue.

Nous aborderons l'installation et la configuration de MSR, la gestion des permissions des utilisateurs de MSR, le renforcement de la sécurité, la certification des images de la registry et l'analyse des scans de sécurité au niveau binaire.

Nous aborderons également la gestion de la registry au travers du garbage collector, de la mise en cache et de l'intégration de webhook.

Les stagiaires recevront de la part de Mirantis une attestation officielle à la fin de la formation.

Public concerné :

- Opérateurs et administrateurs système

Niveau :

- Avancé

Prérequis nécessaires :

- Avoir suivi la formation officielle Docker (Bundle) : Les fondamentaux et Kubernetes Application Essentials ou avoir les connaissances équivalentes.

Connaissances de :

- Linux
- Shell Bash
- Navigation et manipulation du système de fichiers
- Editeurs de texte en ligne de commande comme vim ou nano
- Outils courants tels que curl, wget et ping.
- Notations YAML et JSON.

Objectifs de la formation :

- Exploiter toutes les fonctionnalités de Mirantis Kubernetes Engine afin de gérer en toute sécurité des clusters Kubernetes et Swarm à grande échelle et à utilisateurs multiples.
- Exploiter toutes les fonctionnalités de Mirantis Secure Registry afin d'améliorer le profil de sécurité du contenu, de la distribution et de l'exécution des images de conteneurs.

Matériel pédagogique

En présentiel :

Les formations sont dispensées en présentiel dans des salles de formation équipées d'ordinateurs portables par défaut sous Linux (Ubuntu). Les participants ont accès à internet en wifi ou via des câbles Ethernet.
Le formateur utilise la plateforme d'e-learning Strigo pour dispenser la formation.
Le support de cours est projeté dans la salle de formation via un vidéoprojecteur, remis au stagiaire s'il apporte une clé USB, ou encore envoyé par email après la formation (sur demande).
Le formateur dispose d'un paperboard pour détailler ou insister sur certains aspects.
Un bloc-notes et un stylo sont mis à disposition du participant.

En distanciel :

La formation est dispensée à distance via la plateforme d'e-learning Strigo qui permet de:

- Partager les slides avec les stagiaires
- Accéder à un environnement de lab adapté à la formation
- Une prise en main par le formateur sur chaque environnement de lab si besoin
- Accéder à un streaming, visio/audio, chat
- Avoir une interaction constante avec le formateur
- Accéder à un bloc note pour partager du code

Pédagogie

Les cours théoriques seront dispensés en alternance avec des cas pratiques afin de confronter le participant à diverses situations et lui apprendre à acquérir les bons réflexes et les bonnes pratiques.

Moyens d'encadrement / Suivi de l'exécution de l'action

- Le programme de la formation est remis aux participants avant leur inscription
- Une attestation de formation est établie et transmise au participant quelques jours après la formation.

Évaluation

Chaque participant évalue son parcours de formation avec les travaux pratiques proposés.

Un questionnaire de satisfaction est complété par les participants (avec et sans le formateur afin de leur laisser la possibilité d'exprimer librement leurs remarques) en fin de formation. Cette évaluation est ensuite adressée au commercial en charge du client afin qu'il en prenne connaissance et puisse mesurer la satisfaction client.

PROGRAMME DES 2 JOURS – FORMATION OFFICIELLE DOCKER (BUNDLE) : MKE + MSR

MIRANTIS KUBERNETES ENGINE

Architecture Mirantis Kubernetes Engine

- Patterns de déploiement de production
- Composants conteneurisés de MKE
- Exigences de configuration réseau et système pour MKE
- Installation de MKE via Launchpad pour une haute disponibilité

Contrôle d'accès au MKE

- Systèmes RBAC MKE
- PKI, Client bundle et authentification API
- Comparaison des contrôles d'accès Swarm et Kubernetes

Caractéristiques des réseaux L7

- Interlock pour Swarm
- Istio pour Kubernetes
- Sticky Sessions, déploiements canary ou blue/green, et utilisation de cookies pour les deux orchestrateurs.

MKE Support Dumps

- Générer et comprendre les MKE Support Dumps
- Trouver les informations critiques dans les Dumps pour dépanner MKE
- Activation et Exportation des logs d'audit de l'API pour l'analyse post-mortem

MKE Troubleshooting

- Corrélation entre les événements MKE et les composants
- Parcourir et analyser les fichiers d'état de MKE
- Relance des managers des MKE défaillants
- Sauvegarde et restauration de MKE
- Reprise après incident en cas de défaillance critique du MKE

MIRANTIS SECURE REGISTRY

Architecture Mirantis Secure Registry

- Patterns de déploiement pour la production
- Composants conteneurisés du MSR
- Exigences pour les configurations réseau et système pour MSR
- Installation de MSR via Launchpad pour une haute disponibilité
- Intégration du stockage externe pour le MSR

Contrôle d'accès dans MSR

- Système MSR RBAC (role based access control)

Content Trust

- Déjouer les attaques de type "man in the middle" avec The Update Framework (TUF) et Notary
- Utilisation de Content Trust dans MSR

Analyse de sécurité

- Audit des images de conteneurs pour les vulnérabilités connues
- Configuration de l'analyse de sécurité MSR
- Intégration des scans de sécurité dans l'intégration continue

Automatisation du Repository

- Architecture de pipeline d'intégration continue avec MSR
- Promouvoir et mettre en miroir les images à travers de pipelines
- Intégration de MSR avec des outils externes via des webhooks

Gestion des images

- Stratégies et automatisation de suppression d'image et du "Garbage Collector"
- Stratégie de dimensionnement du Registry
- Mise en cache du contenu pour les équipes réparties sur des zones géographiques différentes

MSR Troubleshooting

- Corrélation des événements de MSR avec les composants
- Lecture et analyse des log d'état de MSR
- Relance des réplicas MSR ayant échoué
- Sauvegardes et restauration de MSR
- Reprise après incident en cas de défaillance critique du MSR