EMGS GROUP
CONSULTING | RECRUITMENT | TRAINING

Contact
☎ 01 75 43 05 58
✉ training@emgsgroup.com

Administrer la plateforme Hadoop 2.X Hortonworks - sécurité

Code formation : EMPHS
Durée : 3 jours – 21h de cours
Format : Inter-entreprise*

3 jours
21 heures de cours

**Cette formation est également disponible en « Intra-entreprise », nous contacter pour plus d'infos.*

| Description

Cette formation est destinée aux administrateurs de la plateforme HDP qui souhaiteraient approfondir leurs connaissances en matière de sécurité. Le focus est mis sur les outils permettant de sécuriser la plateforme en termes d'authentification, d'autorisation et d'audit.

| Objectifs pédagogiques

- Introduire les 5 piliers de la sécurité
- Décrire la façon dont la sécurité est intégrée à Hadoop
- Découvrir et installer Kerberos
- Protéger son cluster avec Knox
- Gérer les permissions et l'audit avec Ranger

| Publics

Administrateur et architecte de la plateforme HDP cherchant à approfondir et à développer leurs compétences

| Pré-requis

- Avoir suivi la formation "Administrer la plateforme Hadoop 2.X Hortonworks 1" serait un plus.
- Expérience en ligne de commande.
- Expérience en administration de la HDP.

| Méthode pédagogique

Formation avec apports théoriques, échanges sur les contextes des participants et retours d'expérience pratique du formateur, complétés de travaux pratiques et de mises en situation.

| Programme détaillé

Jour 1 à 3

- **Décrire les 5 piliers d'un environnement sécurisé**
- **Lister les besoins pour un environnement Hadoop sécurisé**
- **Découvrir comment la sécurité est intégrée dans Hadoop**
- **Choisir vos outils de sécurité en fonction de vos usages**
- **Lister les prérequis de la sécurité**
- **Configurer Kerberos via Ambari**
- **Configurer Kerberos pour Hadoop**
- **Savoir activer Kerberos**
- **Installer et configurer Knox**
- **Installer et configurer ranger**
- **Installer et configurer le ranger key management services (kms)**
- **Utiliser ranger pour sécuriser l'accès aux données**
- **Lister les solutions disponibles des partenaires**
- **Mises en pratique :**
  - Activer l'intégration entre l'OS et AD/LDAP
  - Configurer l'utilisateur du daemon Ambari en non-root
  - Crypter la base de données Ambari
  - Activer l'authentification AD/LDAP sur Ambari
  - Activer HTTPS/SSL pour Ambari
  - Configurer le Two-Way SSL entre les agents Ambari et le serveur
  - Activer l'authentication SPNEGO pour Hadoop
  - Configurer les Ambari Views pour Kerberos
  - Installer Knox par Ambari
  - Configurer la passerelle Knox
  - Configurer Knox pour l'authentification LDAP/AD
  - Installer Ranger via Ambari
  - Configurer Ranger
  - Configurer Ranger KMS
  - Configurer HDFS pour le cryptage des données
  - Configurer Hive pour le cryptage HDFS
  - Activer l'audit sur le Ranger KMS
  - Utiliser le Ranger KMS
  - Tester les accès sécurisés via HDFS, Hive, Pig et Sqoop