DOCAPOSTE Institute

Formation Splunk Analyse des données opérationnelles

Présentation

Ce programme de formation sur Splunk couvre l'installation et la configuration de Splunk, l'indexation de fichiers, et l'exploration de données via des requêtes SPL. Il inclut également la création de tableaux de bord, le développement d'applications, l'utilisation de modèles de données, et la gestion des alertes. Chaque module est accompagné de travaux pratiques pour une application concrète des concepts appris.

Durée : 21,00 heures (3 jours)
Tarif INTRA : Nous consulter

Objectifs de la formation

À l'issue de la formation, le participant sera en mesure de :

- Utiliser Splunk pour collecter, analyser et générer des rapports sur les données
- Enrichir les données opérationnelles à l'aide de recherches et de flux
- Créer des alertes en temps réel, scriptées et d'autres alertes intelligentes
- Intégrer des graphiques JavaScript avancés
- Utiliser l'API de Splunk

Prérequis

Connaissances de base en logs et sécurité

Public

Administrateurs, ingénieurs système

Programme de la formation

Configurer Splunk

- L'obtention d'un compte Splunk.com
- Installer Splunk sous Windows

Docaposte Institute
ACI 3A3-303 - 45-47 Boulevard Paul Vaillant Couturier, 94200 IVRY SUR SEINE
Tél : Variable non renseignée - Email : hello.institute@docaposte.fr
SIRET : 813 058 542 00032 - Code APE : 8559A - N TVA Intra : FR 58 813 058 542
Déclaration d'activité enregistrée sous le numéro 11941117994 auprès du préfet de région d'Ile-de-France

- Indexer des fichiers et des répertoires via l'interface Web, CLI, par fichiers de configuration

Travaux pratiques : Configurer Splunk. Mise en œuvre de définition d'extractions de champs, de types d'évènements et de labels.

Exploration de données

- Requêtes de SPL. Opérateurs booléens, commandes
- Recherche à l'aide de plages de temps

Travaux pratiques : Extraire des fichiers de journalisation, les pages Web les plus visitées, le navigateur le plus utilisé, les sites les plus visités...

Tableaux de bord

- Les tableaux de bord et l'intelligence opérationnelle, faire ressortir les données. Les types de graphes.

Travaux pratiques : Créer, enrichir un tableau de bord avec des graphes liés aux recherches réalisées.

Nouvelle application

- Installer une application existante issue de Splunk ou d'un tiers
- Ajouter des tableaux de bord et recherches à une application
- Tableaux de bord interactifs
- Produire de façon régulière (programmée) des tableaux de bord au format PDF

Travaux pratiques : Créer une nouvelle application Splunk. Installer une application et visualiser des événements liés aux switchs Cisco.

Modèles de données

- Les modèles de données
- Mettre à profit des expressions régulières
- Optimiser la performance de recherche
- Pivoter des données

Travaux pratiques : Utiliser la commande pivot, des modèles pour afficher les données.

Types d'alertes

- Conditions surveillées.

Docaposte Institute
ACI 3A3-303 - 45-47 Boulevard Paul Vaillant Couturier, 94200 IVRY SUR SEINE
Tél : Variable non renseignée - Email : hello.institute@docaposte.fr
SIRET : 813 058 542 00032 - Code APE : 8559A - N TVA Intra : FR 58 813 058 542
Déclaration d'activité enregistrée sous le numéro 11941117994 auprès du préfet de région d'Ile-de-France

- Actions entreprises suite à alerte avérée.
- Devenir proactif avec les alertes.

Travaux pratiques : Exécuter un script quand se produit l'erreur de serveur Web 503, écrire les détails associés à l'événement dans un fichier.

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 compétences.

Moyens pédagogiques et techniques

- Apports des connaissances communes.
- Mises en situation sur le thème de la formation et des cas concrets.
- Méthodologie d'apprentissage attractive, interactive et participative.
- Equilibre théorie / pratique : 60 % / 40 %.
- Supports de cours fournis au format papier et/ou numérique.
- Ressources documentaires en ligne et références mises à disposition par le formateur.
- Pour les formations en présentiel dans les locaux mis à disposition, les apprenants sont accueillis dans une salle de cours équipée d'un réseau Wi-Fi, d'un tableau blanc ou paperboard. Un ordinateur avec les logiciels appropriés est mis à disposition (le cas échéant).

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

En amont de la formation :

- Recueil des besoins des apprenants afin de disposer des informations essentielles au bon déroulé de la formation (profil, niveau, attentes particulières...).
- Auto-positionnement des apprenants afin de mesurer le niveau de départ.

Docaposte Institute
ACI 3A3-303 - 45-47 Boulevard Paul Vaillant Couturier, 94200 IVRY SUR SEINE
Tél : Variable non renseignée - Email : hello.institute@docaposte.fr
SIRET : 813 058 542 00032 - Code APE : 8559A - N TVA Intra : FR 58 813 058 542
Déclaration d'activité enregistrée sous le numéro 11941117994 auprès du préfet de région d'Ile-de-France

Tout au long de la formation :

- Évaluation continue des acquis avec des questions orales, des exercices, des QCM, des cas pratiques ou mises en situation...

A la fin de la formation :

- Auto-positionnement des apprenants afin de mesurer l'acquisition des compétences.
- Evaluation par le formateur des compétences acquises par les apprenants.
- Questionnaire de satisfaction à chaud afin de recueillir la satisfaction des apprenants à l'issue de la formation.
- Questionnaire de satisfaction à froid afin d'évaluer les apports ancrés de la formation et leurs mises en application au quotidien.

Accessibilité

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

Docaposte Institute
ACI 3A3-303 - 45-47 Boulevard Paul Vaillant Couturier, 94200 IVRY SUR SEINE
Tél : Variable non renseignée - Email : hello.institute@docaposte.fr
SIRET : 813 058 542 00032 - Code APE : 8559A - N TVA Intra : FR 58 813 058 542
Déclaration d'activité enregistrée sous le numéro 11941117994 auprès du préfet de région d'Ile-de-France