+33 (0)1 48 10 09 46
formation@ambient-it.net
140 Avenue Jean Lolive 93500 Pantin - France

Mis à jour le 24/06/2025

S'inscrire

Formation Splunk

3 jours (21 heures)

Présentation

L'entreprise fut fondée en 2003 par les co-fondateurs Erik Swan, Rob Das et Michael Baum, trois serials entrepreneur de la Silicon Valley. Le nom « Splunk » fait référence à l'exploration de caves et à sa pratique qui porte le nom anglais de « spelunking ». Ainsi, le nom réfère à leur plongeon dans le profond et nouveau domaine qu'est le Big Data.

Splunk 8 collecte et analyse en temps réel d'importants volumes de données générées par des machines. Elle utilise une API standard permettant une connexion directe du service vers les applications et les appareils. Il permet de générer des graphiques, des rapports, des alertes, des tableaux de bord et des infographies.

Splunk propose des produits qui réalisent des recherches d'historiques en temps réel afin d'extraire des analyses statistiques et tableau de bord, pour l'aide à la décision. Le logiciel peut indexer des données machines structurées ou non-structurées. Les recherches et analyses sont effectuées grâce à un langage de recherche propre à Splunk.

Ce langage englobe toutes les commandes de recherche et leurs fonctions. Sa syntaxe a été fondée sur une base UNIX et SQL, elle comprend la recherche de données, le filtrage, la modification, manipulation, insertion et suppression. Nous vous enseignerons, bien sûr, la dernière version de l'outil en date à savoir Splunk 9.4.

Objectifs

- Maîtriser les principes de Splunk
- Savoir gérer des données machines
- Créer des tableaux de bord statistiques

Public visé

- Développeurs
- Architectes
- Administrateurs

Pré-requis

Connaissances dans le Big Data et la Data Analytics

PROGRAMME DE NOTRE FORMATION SPLUNK

Introduction à Splunk

- Qu'est-ce que Splunk ?
- Présentation de l'architecture
- Installation de Splunk
- Paramétrage

Créer des applications Splunk

- Choix de l'architecture
- Créer son app Splunk
- Surveiller les logs
- Améliorer les performances de l'application
- Packager l'app

Recherches et données

- Les données
  - Splunk Web
  - Identifier les types d'entrée
  - Ajouter et accéder aux données
- Utilisation de l'option moniteur
- La recherche
  - Exécuter des recherche de base
  - La saisie automatique
  - Les intervalles de recherche
  - Utilisation de la ligne du temps
- Enregistrer les résultats de recherche
- Utiliser les fields
- Introduction aux SPL
- Les pipelines
- Les tables, les champs et les commandes

Pivot

- Qu'est-ce qu'un pivot ?
- La relation entre data model et pivot
- Sélectionner un objet de data model
- Créer un rapport pivot
- Le pivot instantané

Rapports et tableau de bord

- Présentation de l'interface et des éléments
- Les bonnes pratiques de Data Visualization
- Quel type de vue utilisé ?
- SplunkJS dashboard
- Utilisation des tokens
- Les event handlers
- Les bonnes pratiques de sécurité

Rest API

- Introduction
- Les différents niveaux d'autorisations
- Utiliser les index
- HTTP Event Collector (**HEC**)
- Recherche avancée
- Job management

Sociétés concernées

Cette formation s’adresse à la fois aux particuliers ainsi qu’aux entreprises, petites ou grandes, souhaitant former ses équipes à une nouvelle technologie informatique avancée ou bien à acquérir des connaissances métiers spécifiques ou des méthodes modernes.

Positionnement à l'entrée en formation

Le positionnement à l'entrée en formation respecte les critères qualité Qualiopi. Dès son inscription définitive, l'apprenant reçoit un questionnaire d’auto-évaluation nous permettant d’apprécier son niveau estimé sur différents types de technologies, ses attentes et objectifs personnels quant à la formation à venir, dans les limites imposées par le format sélectionné. Ce questionnaire nous permet également d’anticiper certaines difficultés de connexion ou de sécurité interne en entreprise (intraentreprise ou classe virtuelle) qui pourraient être problématiques pour le suivi et le bon déroulement de la session de formation.

Méthodes pédagogiques

Stage Pratique : 60% Pratique, 40% Théorie. Support de la formation distribué au format numérique à tous les participants.

Organisation

Le cours alterne les apports théoriques du formateur soutenus par des exemples et des

séances de réflexions, et de travail en groupe.

Validation

À la fin de la session, un questionnaire à choix multiples permet de vérifier l'acquisition correcte des compétences.

Sanction

Une attestation sera remise à chaque stagiaire qui aura suivi la totalité de la formation.

Organisme de formation enregistré sous le numéro 11 75 54743 75. Cet enregistrement ne vaut pas agrément de l'État.
© Ambient IT 2015-2025. Tous droits réservés. Paris, France - Suisse - Belgique - Luxembourg