Splunk Enterprise Administration Fast Start (ADM-FT)

ID ADM-FT **Prix** CHF 4 200,– (Hors Taxe) **Durée** 5 jours

A qui s'adresse cette formation

- Cette formation s’adresse aux administrateurs systèmes et aux administrateurs en charge de la gestion d’un environnement Splunk Enterprise.
- Elle fournit les connaissances fondamentales sur le license manager, les indexers et les search heads.
- Elle couvre également les bases des forwarders Splunk et les méthodes d’ingestion de données distantes vers les indexers.

Cette formation prépare à la/aux certifications

Splunk Enterprise Certified Admin (SECA)

Pré-requis

Splunk Power User Fast Start (POWER-U)

Objectifs

À l’issue de cette formation, vous serez en mesure de :

- Comprendre l’administration système
- Comprendre le déploiement Splunk
- Comprendre la gestion des licences
- Comprendre les applications Splunk
- Comprendre les fichiers de configuration Splunk
- Comprendre les utilisateurs, rôles et mécanismes d’authentification
- Ingérer des données dans Splunk (Get Data In)
- Comprendre la recherche distribuée (Distributed Search)
- Comprendre l’administration des données
- Comprendre les sourcetypes
- Gérer et déployer des forwarders
- Configurer les entrées de données (data inputs)
- Comprendre les file monitors
- Comprendre les entrées réseau (TCP/UDP)
- Comprendre les entrées scriptées
- Comprendre les entrées HTTP (via le HTTP Event Collector)
- Personnaliser le processus de parsing lors de la phase d’ingestion
- Définir des transformations pour modifier les données avant indexation
- Définir les configurations des knowledge objects au moment de la recherche

Contenu

Splunk Enterprise System Administration

Module 1 - Déploiement du serveur Splunk

- Présenter une vue d’ensemble de Splunk
- Identifier les composants de Splunk Enterprise
- Identifier les types de déploiement Splunk
- Lister les étapes d’installation de Splunk
- Utiliser les commandes CLI de Splunk

Module 2 - Splunk Server Monitoring

- Activer la Monitoring Console (MC)
- Identifier les types de licences Splunk
- Comprendre les violations de licence
- Ajouter et supprimer des licences
- Utiliser Splunk Diag

Module 3 - Applications Splunk

- Décrire les apps et add-ons Splunk
- Installer une application sur une instance Splunk
- Gérer l’accessibilité et les permissions des applications

Module 4 - Fichiers de configuration Splunk

- Décrire la structure des répertoires de configuration
- Comprendre le mécanisme de superposition des configurations (configuration layering)
- Utiliser btool pour analyser les paramètres de configuration

Module 5 - Splunk Indexes

- Comprendre le fonctionnement des index Splunk
- Identifier les types de index buckets
- Créer et manipuler des index
- Vue d’ensemble des metrics index

Module 6 - Gestion des index Splunk

- Revoir les fondamentaux de la gestion des index
- Identifier les bonnes pratiques de rétention des données
- Identifier les recommandations de sauvegarde
- Déplacer et supprimer des données d'index
- Comprendre l'utilisation du Fishbucket
- Restaurer un frozen bucket

Module 7 - Gestion des utilisateurs Splunk

- Ajouter des utilisateurs via l'authentification native
- Comprendre les rôles utilisateurs dans Splunk
- Créer un rôle personnalisé
- Gérer les utilisateurs

Module 8 - Configuration du forwarding de base

- Identifier les étapes de configuration des forwarders
- Configurer un Universal Forwarder
- Comprendre le Deployment Server

Module 9 - Recherche distribuée

- Comprendre le fonctionnement de la recherche distribuée
- Définir les rôles du search head et des search peers

Splunk Enterprise Data Administration

Module 1 - Introduction à l'administration des données

- Présenter une vue d'ensemble de Splunk
- Décrire les quatre phases du modèle distribué
- Décrire les types d'entrées de données et les paramètres de métadonnées
- Configurer des tests d'ingestion initiaux via Splunk Web
- Tester les index avec l'Input Staging

Module 2 - Ingestion des données – Staging

- Identifier les fichiers et répertoires de configuration Splunk
- Comprendre la priorité entre index-time et search-time
- Valider et mettre à jour les fichiers de configuration

Module 3 - Configuration des forwarders

- Identifier le rôle des indexers de production et des forwarders
- Comprendre et configurer les Universal Forwarders
- Comprendre et configurer les Heavy Forwarders
- Comprendre et configurer les forwarders intermédiaires
- Identifier les options supplémentaires des forwarders

Module 4 - Gestion des forwarders

- Comprendre le Splunk Deployment Server (DS)
- Gérer les forwarders via des deployment apps
- Configurer les clients de déploiement et les groupes de clients
- Superviser les activités de gestion des forwarders

Module 5 - Entrées de type Monitor

- Créer des entrées de surveillance de fichiers et répertoires
- Utiliser les paramètres optionnels des monitor inputs
- Déployer un monitor input distant

Module 6 - Entrées réseau et scriptées

- Créer des entrées réseau (TCP et UDP)
- Décrire les options avancées des entrées réseau

Module 7 - Entrées sans agent (Agentless)

- Créer une entrée scriptée simple

Module 8 - Optimisation des entrées

- Configurer le HTTP Event Collector (HEC) pour des entrées sans agent
- Présenter le Splunk App for Stream

Module 9 - Phase de parsing et données

- Identifier les entrées spécifiques Linux
- Identifier les entrées spécifiques Windows

Module 10 - Manipulation des données brutes

- Comprendre le traitement par défaut lors de la phase d'ingestion
- Configurer les options de parsing (sourcetype, encodage des caractères, etc.)

Module 11 - Knowledge Objects associés

- Comprendre le traitement par défaut lors du parsing
- Optimiser et configurer le découpage des événements (line breaking)
- Comprendre l'extraction et l'affectation des timestamps et fuseaux horaires
- Utiliser Data Preview pour valider la création des événements

Module 12 - Création d'un Diag

- Comprendre la définition et l'utilisation des transformations de données
- Utiliser les transformations via props.conf et transforms.conf pour :

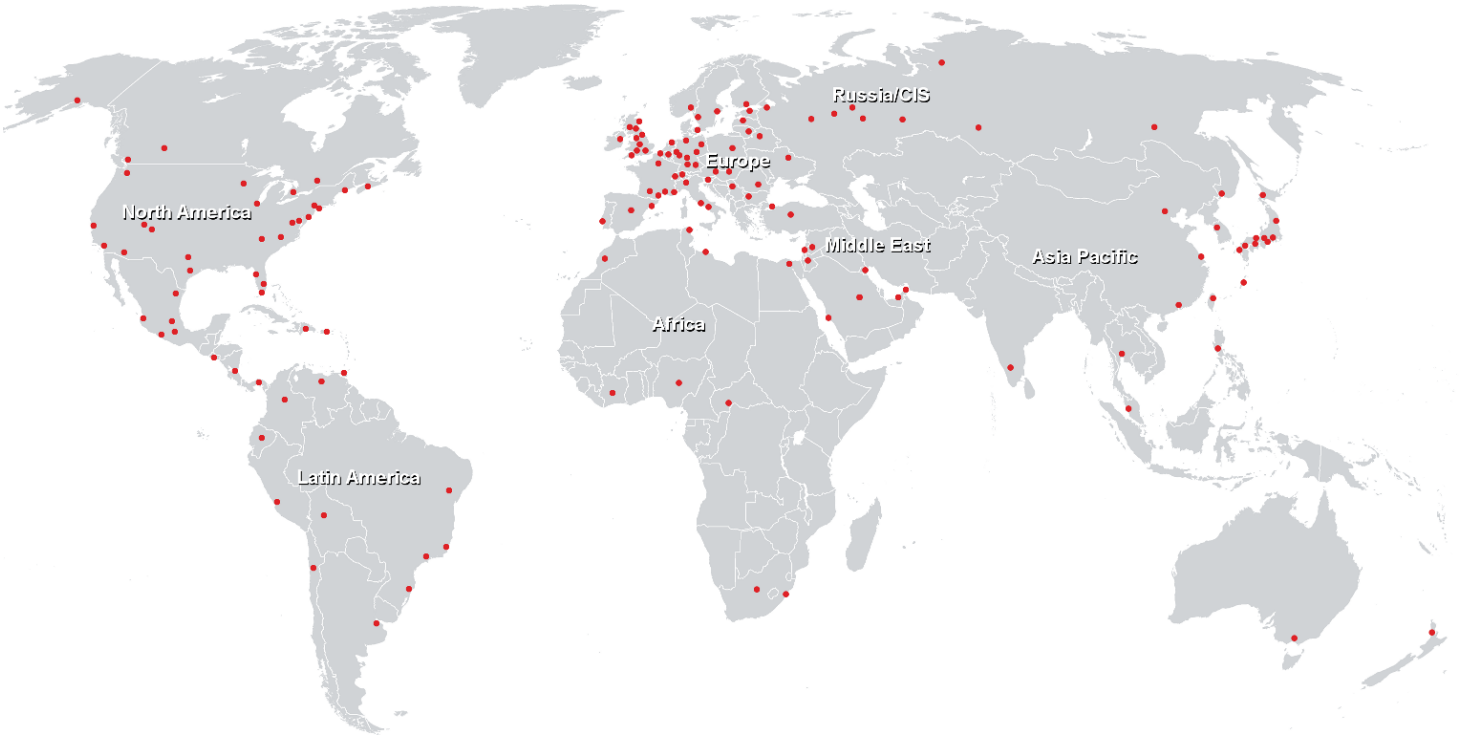
- Masquer ou supprimer des données lors de l’indexation
- Redéfinir le sourcetype ou le host selon le contenu des événements
- Router les événements vers des index spécifiques
- Empêcher l’indexation d’événements non souhaités
- Utiliser SEDCMD pour modifier les données brutes

Module 13 - Knowledge Objects associés

- Définir les extractions de champs par défaut et personnalisées (search time)
- Identifier les avantages et inconvénients des extractions au moment de l’indexation
- Configurer les extractions de champs indexés
- Comprendre les extractions par défaut au moment de la recherche
- Gérer les knowledge objects orphelins

Splunk Enterprise Administration Fast Start (ADM-FT)

Centres de formation dans le monde entier





Fast Lane Institute for Knowledge Transfer (Switzerland) AG

Husacherstrasse 3
CH-8304 Wallisellen
Tel. +41 44 832 50 80

info@flane.ch, https://www.flane.ch