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

- This course is designed for system administrators and administrators who are responsible for managing the Splunk Enterprise environment.
- The course provides the fundamental knowledge of Splunk license manager, indexers and search heads.
- The course provides the fundamental knowledge of Splunk forwarders and methods to get remote data into Splunk indexers.

Cette formation prépare à la/aux certifications

Splunk Enterprise Certified Admin (SECA)

Pré-requis

Splunk Power User Fast Start (POWER-U)

Objectifs

At the end of this course, you should be able to :

- Understand System Administration
- Understand Splunk Deployment
- Understand License Management
- Understand Splunk Apps
- Understand Splunk Configuration Files
- Understand Users, Roles, and Authentication
- Get Data In
- Understand Distributed Search
- Understand Data Administration
- Understand sourcetypes
- Manage and deploy forwarders
- Configure data inputs
- Understand Fire monitors
- Understand Network inputs (TCP/UDP)
- Understand Scripted inputs
- Understand HTTP inputs (via the HTTP Event Collector)
- Customize the input phase parsing process
- Define transformations to modify data before indexing
- Define search time knowledge object configurations

Contenu

Splunk Enterprise System Administration

Module 1 - Splunk Server Deployment

- Provide an overview of Splunk
- Identify Splunk Enterprise components
- Identify the types of Splunk deployments
- List the steps to install Splunk
- Use Splunk CLI commands

Module 2 - Splunk Server Monitoring

- Enable the Monitoring Console (MC)
- Identify Splunk license types
- Describe license violations
- Add and remove licenses
- Use Splunk Diag

Module 3 - Splunk Apps

- Describe Splunk apps and add-ons
- Install an app on a Splunk instance
- Manage app accessibility and permissions

Module 4 - Splunk Configuration Files

- Describe Splunk configuration directory structure
- Understand configuration layering process
- Use btool to examine configuration settings

Module 5 - Splunk Indexes

- Learn how Splunk indexes function
- Identify the types of index buckets
- Add and work with indexes
- Overview of metrics index

Module 6 - Splunk Index Management

- Review Splunk Index Management basics
- Identify data retention recommendations
- Identify backup recommendations
- Move and delete index data
- Describe the use of the Fishbucket
- Restore a frozen bucket

Module 7 - Splunk User Management

- Add Splunk users using native authentication
- Describe user roles in Splunk
- Create a custom role
- Manage users in Splunk

Module 8 - Configuring Basic Forwarding

- Identify forwarder configuration steps
- Configure a Universal Forwarder
- Understand the Deployment Server

Module 9 - Distributed Search

- Describe how distributed search works
- Define the roles of the search head and search peers

Splunk Enterprise Data Administration

Module 1 -Introduction to Data Administration

- Provide an overview of Splunk
- Describe the four phases of the distributed model
- Describe data input types and metadata settings
- Configure initial input testing with Splunk Web
- Testing Indexes with Input Staging

Module 2 - Getting Data In - Staging

- Identify Splunk configuration files and directories
- Describe index-time and search-time precedence
- Validate and update configuration files

Module 3 - Configuring Forwarders

- Identify the role of production indexers and forwarders
- Understand and configure Universal Forwarders
- Understand and configure Heavy Forwarders
- Understand and configure intermediate forwarders
- Identify additional forwarder options

Module 4 - Forwarder Management

- Describe Splunk Deployment Server (DS)
- Manage forwarders using deployment apps
- Configure deployment clients and client groups
- Monitor forwarder management activities

Module 5 - Monitor Inputs

- Create file and directory monitor inputs
- Use optional settings for monitor inputs
- Deploy a remote monitor input

Module 6 - Network and Scripted Inputs

- Create network (TCP and UDP) inputs
- Describe optional settings for network inputs

Module 7 - Agentless Inputs

- Create a basic scripted input

Module 8 - Fine Tuning Inputs

- Configure Splunk HTTP Event Collector (HEC) agentless input
- Describe Splunk App for Stream

Module 9 - Parsing Phase and Data

- Identify Linux-specific inputs
- Identify Windows-specific inputs

Module 10 - Manipulating Raw Data

- Understand the default processing that occurs during input phase
- Configure input phase options, such as source type fine-tuning and character set encoding

Module 11 - Supporting Knowledge Objects

- Understand the default processing that occurs during parsing
- Optimize and configure event line breaking
- Explain how timestamps and time zones are extracted or assigned to events
- Use Data Preview to validate event creation during parsing phase

Module 12 - Creating a Diag

- Explain how data transformations are defined and invoked
- Use transformations with props.conf and transforms.conf to:
- Mask or delete raw data as it is being indexed
- Override sourcetype or host based upon event values
- Route events to specific indexes based on event content
- Prevent unwanted events from being indexed
- Use SEDCMD to modify raw data

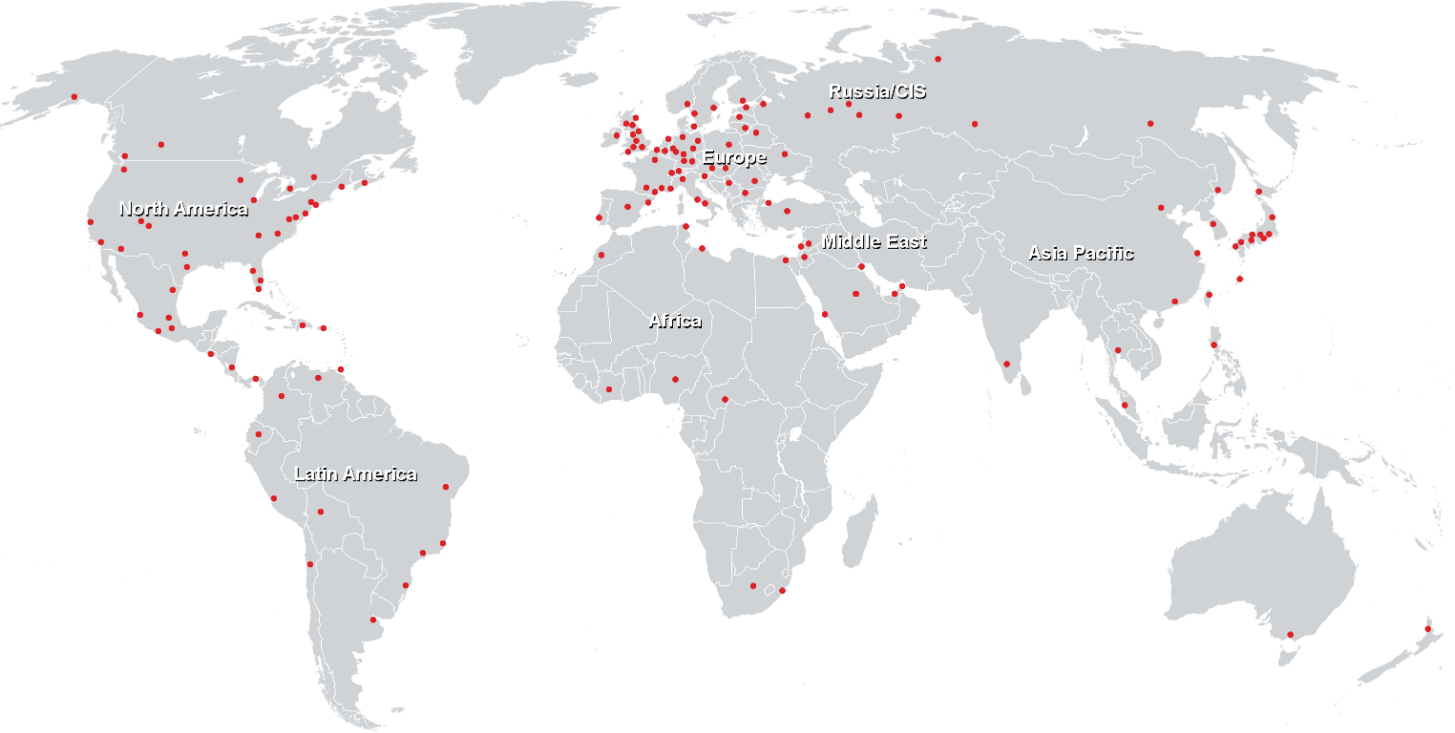
Module 13 - Supporting Knowledge Objects

- Define default and custom search time field extractions
- Identify the pros and cons of indexed time field extractions
- Configure indexed field extractions
- Describe default search time extractions

- Manage orphaned knowledge object

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