Splunk Enterprise Architect Fast Start (ARCH-FT)

ID ARCH-FT **Prix** CHF 4 400,– (Hors Taxe) **Durée** 5 jours

A qui s'adresse cette formation

Splunk administrators Eexperienced Splunk Enterprise administrator who is new to Splunk Clusters

Cette formation prépare à la/aux certifications

Splunk Enterprise Certified Architect (SPECA)

Pré-requis

Splunk Core Certified Power User AND Splunk Enterprise Certified Admin.

Hard pre-req: The three ILTs in this path PLUS the Splunk Enterprise Practical Lab.

Objectifs

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

- Understand Splunk Troubleshooting Methods and Tools
- Index Problems
- Input Configuration Problems
- Understand Deployment Problems
- Understand License, Upgrade, and User Management Problems
- Understand Search Management Problems
- User Search Problems
- Understand the Splunk Support Model and its resources
- Identify the best practices for troubleshooting Splunk Enterprise
- List ways to gather useful Splunk diagnostic information
- Use Splunk diagnostic tools
- Identify common Splunk technical issues and solve them
- Understand Requirements definition
- Understand Index and resource planning
- Understand Cluster
- Understand Forwarder and Deployment
- Integration
- Understand Performance Monitoring and Tuning
- Understand Large-scale Splunk Deployment
- Understand Single-site Indexer Cluster
- Understand Indexer Cluster Management and Administration
- Understand Forwarder Configuration
- Understand Search Head Cluster
- Understand Search Head Cluster Management and Administration
- Understand KV Store Collection and Lookup Management
- Understand SmartStore Implementation

Contenu

Troubleshooting Splunk Enterprise

Module 1 – Splunk Troubleshooting Methods and Tools

- Describe the Splunk Troubleshooting Approach
- List Splunk Diagnostic Resources and Tools
- Create and Splunk a Diag
- Use RapidDiag

Module 2 – Indexing Problems

- Discover Splunk Deployment Topology and its Server Roles
- Identify Where to Check the Index-Time Pipeline Status
- Use the metrics.log to Clarify the Index-Time Problem

Module 3 – Input Configuration Problems

- Data Input Issues
- Troubleshooting Inputs with the Monitoring Console

Module 4 – Deployment and Forwarder Problems

- Deployment Server Issues
- Forwarding and Receiving Issues

Module 5 – License, Upgrade, and User Management Problems

- Installation Issues
- Upgrade Considerations
- Splunk Licensing Issues
- Splunk Roles and User Management Issues

Module 6 – Search Head Management Problems

- Troubleshoot Distributed Search Issues
- Identify Job Scheduling Problems
- Learn to Diagnose Crashing Problems
- Describe How to Prioritize Resources for Critical Splunk Processes

Module 7 – User Search Problems

- Identify the Types of Search Problems
- Isolate and Troubleshoot Search Problems

Splunk Enterprise Cluster Administration

Module 1 – Splunk Troubleshooting Methods and Tools

- Deployment Design Factors
- How Splunk Enterprise can scale
- Splunk License Master
- Splunk 9.0 Security

Module 2 – Single-site Indexer Cluster

- How Splunk Single-Site Indexer Clusters Work
- Indexer Cluster Components and Terms
- Splunk single-site Indexer Cluster Configuration
- Splunk Indexer Cluster Log Channels

Module 3 – Multisite Indexer Cluster

- How Splunk Multisite Indexer Clusters Work
- Multisite Indexer Cluster Terms
- Multisite Indexer Cluster Configuration
- Optional Multisite Indexer Cluster Configurations

Module 4 – Indexer Cluster Management and Administration

- Peer Offline and Decommission
- Master App Bundles
- Indexer Cluster Storage Utilization Options
- Site Mapping
- Monitoring Console for Indexer Cluster Environment
- Cluster Manager Redundancy

Module 5 – Forwarder Management

- Indexer Discovery
- Optional Indexer Discovery Configurations
- Volume-Based Forwarder Load Balancing

Module 6 – Search Head Cluster

- Search Head Cluster Architecture
- Search Head Cluster Configuration
- Captaincy Identification and Cluster Status
- Search Head Cluster Settings

Module 7 – Search Head Cluster Management

- Search Head Cluster Deployer
- Captaincy Transfer
- Search Head Member Addition and Decommissioning
- Monitoring Console for Search Head Cluster

Module 8 – KV Store Collection and Lookup Management

- KV Store Collection in Splunk Clusters
- KV Store Monitoring with Monitoring Console

Module 9 – Introduction to Smart Store

- SmartStore Deployment Use Cases
- SmartStore Architecture Overview
- Enable SmartStore in Indexer Cluster
- Monitor SmartStore Status

Architecting Splunk Enterprise Deployments

Module 1 – Introduction

- Overview of the Splunk deployment planning process and associated tools

Module 2 – Project Requirements

- Identify critical information about environment, volume, users, and requirements
- Review checklists and resources to aid in collecting requirements

Module 3 – Infrastructure Planning: Index Design

- Design and size indexes
- Estimate storage requirements
- Identify relevant apps

Module 4 – Infrastructure Planning: Resource Planning

- List sizing factors for servers
- Describe how reference hardware is used to scale deployments
- Identify the impact of clustering for index replication and for

search heads

Module 5- Clustering Overview

- Describe the different clustering capabilities
- Introduce the concepts of indexer and search head clustering

Module 6 - Forwarder and Deployment Best Practices

- Review types of forwarders
- Describe how to manage forwarder installation
- Review configuration management for all Splunk components, using Splunk deployment tools
- Provide best practices for a Splunk deployment

Module 7 - Integration

- Describe integration methods
- Identify common integration points

Module 8 – Performance Monitoring and Tuning

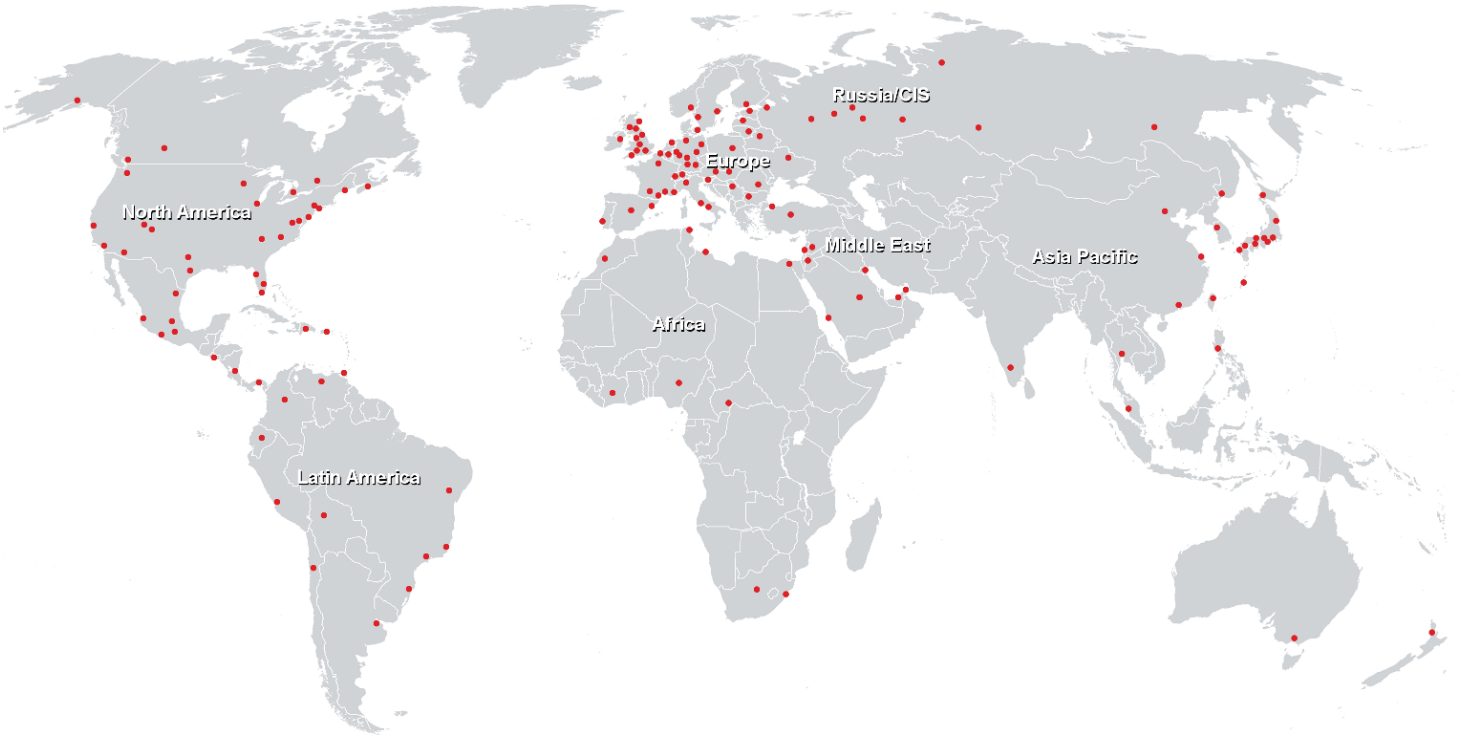
- Use the Monitoring Console to track the performance of your test environment
- List options to fine tune performance for production environment

Module 9 – Use Cases

- Provide example architecture topologies
- Discuss different architecture options based on use case

Splunk Enterprise Architect Fast Start (ARCH-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