Services Core Implementation (SCI)

ID SCI **Prix** CHF 4 000,– (Hors Taxe) **Durée** 5 jours

Pré-requis

- Splunk Certified Architect +

Objectifs

Topic 1 – Deploying Splunk

- Introduce the Splunk Validated Architectures
- Review how Splunk can grow from a standalone environment to a distributed environment with indexer and search head clustering
- Explain High Availability and Disaster Recovery
- Discuss migrating Splunk from on-premises to the Cloud
- Lab 0: Grade Me

Topic 2 – Monitoring Console

- Discuss the best instance to configure as the Monitoring Console
- Configure the MC for a single or distributed environment
- Examine how the MC uses the server roles and groups assigned to instances
- Discuss health checks and how they are run
- Lab 1 - Discovery

Topic 3 – Configuration Management

- Define deployment apps
- Provide overview of Deployment Server
- Describe deployment system configuration
- Discuss how to manage Deployment Server at scale
- Lab 5: Scale DS

Topic 4 – Access & Roles

- Discuss how to manage Deployment Server at scale
- Identify authentication methods
- Describe LDAP concepts and configuration
- Discuss SAML and SSO options
- Define roles and how they are used to protect data
- Lab 2: LDAP Integration

Topic 5 – Data Collection

- Examine Splunk to Splunk (S2S) communication and the different ways data is sent from forwarder to indexer
- Describe the types and configuration of data inputs
- Discuss ways to troubleshoot data inputs
- Lab 3: Triage broken forwarder

Topic 6 – Indexing

- Review indexing artifacts and locations
- Discuss event processing and data pipelines
- Understand the underlying text parsing and indexing process
- Examine data retention controls
- Lab 4: Triage indexing issue

Topic 7 – Search

- Examine the inter-workings of a search
- Discuss how to use search job inspection
- Look at the different search types and how to maximize search efficiency
- Review sub-searches and how they work
- Examine some example searches and how to make them more efficient

Topic 8 – Index Clustering

- Provide an architecture overview
- Describe deployment and component configuration
- Review upgrade strategy
- Discuss data buckets and lifecycle
- Examine failure modes and recovery processes
- Introduce multi-site clustering
- Understand migration procedures
- Lab 6: Upgrade Index Cluster
- Lab 7: Expand Cluster & Migrate Indexer data

Topic 9 – Search Head Clustering

- Provide overview of Search Head clustering
- Explain how to manage and deploy a cluster
- Describe content management using the Deployer
- Review the role of cluster members and the Captain
- Lab 8 – Install SHC

Appendix A – REST API

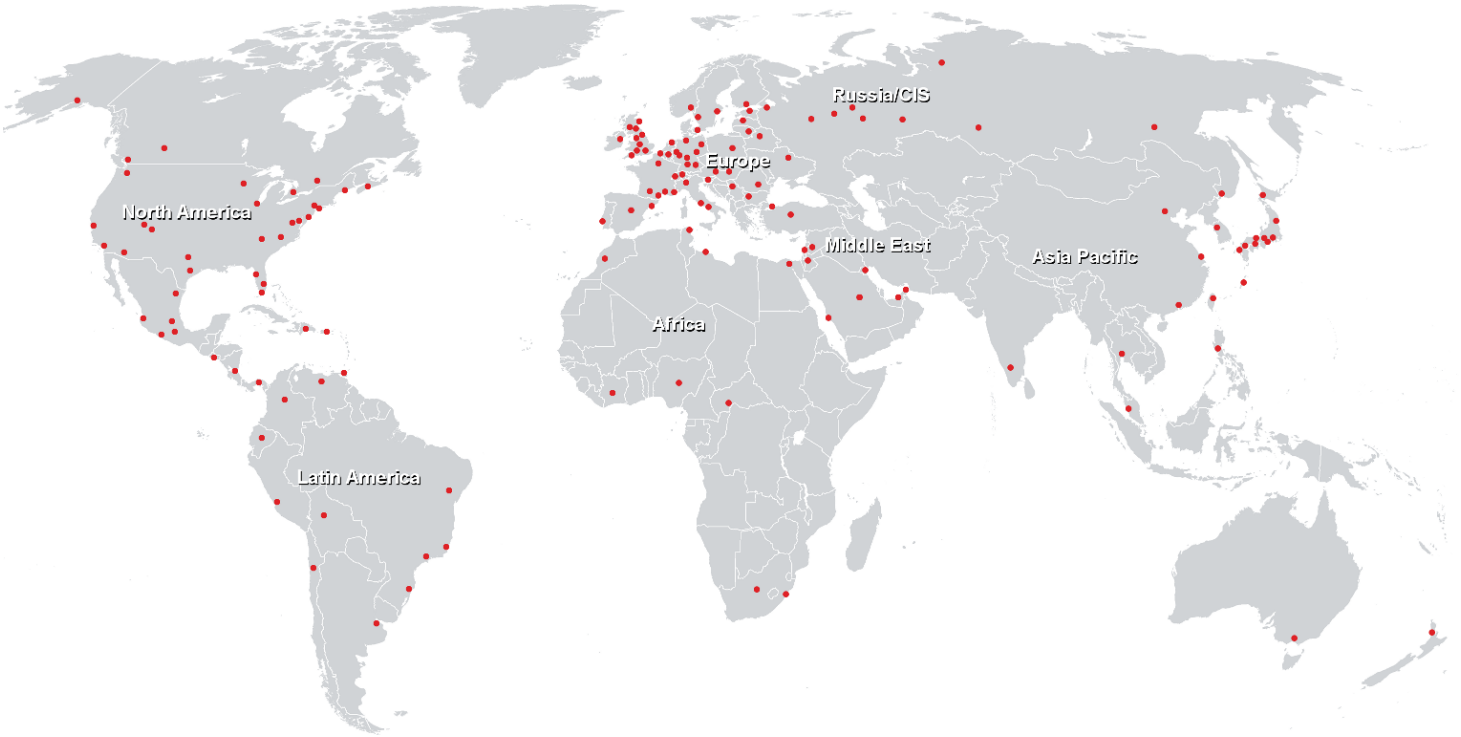
- Define the Splunk REST API
- Discuss requests, endpoints, and namespaces
- Examine tools and methods for using the API

Contenu

- Splunk architecture
- Monitoring Console
- Deployment Server
- LDAP integration
- Collecting and forwarding data
- Indexing and Searching
- Clustering indexers
- Clustering Search Heads

Services Core Implementation (SCI)

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