Services Core Implementation (SCI)

ID SCI **Preis** auf Anfrage **Dauer** 5 Tage

Voraussetzungen

- Splunk Zertifizierter Architekt +

Kursziele

Thema 1 - Bereitstellung von Splunk

- Einführung in die validierten Architekturen von Splunk
- Überprüfen Sie, wie Splunk von einer Standalone-Umgebung zu einer verteilten Umgebung mit Indexer- und Suchkopf-Clustering wachsen kann
- Erklären Sie Hochverfügbarkeit und Disaster Recovery
- Diskussion über die Migration von Splunk von On-Premises in die Cloud
- Labor 0: Klasse Ich

Thema 2 - Überwachungskonsole

- Diskutieren Sie die beste Instanz für die Konfiguration der Überwachungskonsole
- Konfigurieren Sie den MC für eine einzelne oder verteilte Umgebung
- Prüfen Sie, wie der MC die den Instanzen zugewiesenen Serverrollen und -gruppen verwendet
- Diskussion über Gesundheitskontrollen und deren Durchführung
- Labor 1 - Entdeckung

Thema 3 - Konfigurationsmanagement

- Definieren Sie Einsatzanwendungen
- Überblick über den Deployment Server geben
- Beschreiben Sie die Konfiguration des Bereitstellungssystems
- Diskutieren Sie, wie Sie Deployment Server im grossen Massstab verwalten können
- Labor 5: DS-Waagen

Thema 4 - Zugang und Rollen

- Diskutieren Sie, wie Sie Deployment Server im grossen Massstab verwalten können
- Identifizierung von Authentifizierungsmethoden
- Beschreiben Sie LDAP-Konzepte und -Konfiguration
- SAML- und SSO-Optionen besprechen
- Definieren Sie Rollen und wie sie zum Schutz von Daten verwendet werden
- Übung 2: LDAP-Integration

Thema 5 - Datenerhebung

- Untersuchung der Kommunikation von Splunk zu Splunk (S2S) und der verschiedenen Wege, auf denen Daten vom Forwarder zum Indexer gesendet werden
- Beschreiben Sie die Arten und die Konfiguration der Dateneingänge
- Besprechen Sie Möglichkeiten zur Fehlersuche bei Dateneingaben
- Übung 3: Sichtung defekter Forwarder

Thema 6 - Indizierung

- Überprüfung von Indizierungsartefakten und Standorten
- Diskussion über Ereignisverarbeitung und Datenpipelines
- den zugrundeliegenden Prozess der Textanalyse und -indizierung zu verstehen
- Prüfung der Kontrollen zur Datenaufbewahrung
- Übung 4: Sichtung von Indizierungsproblemen

Thema 7 - Suche

- Untersuchung des Zusammenspiels einer Suche
- Diskutieren Sie, wie Sie die Suchauftragsinspektion nutzen können
- Sehen Sie sich die verschiedenen Sucharten an und wie Sie die Sucheffizienz maximieren können
- Überprüfung der Untersuchen und ihrer Funktionsweise
- Untersuchen Sie einige Beispielsuchen und wie Sie diese effizienter gestalten können

Thema 8 - Index-Clustering

- Einen Überblick über die Architektur geben
- Beschreiben Sie den Einsatz und die Konfiguration der Komponenten
- Überprüfung der Upgrade-Strategie
- Diskussion über Dateneimer und Lebenszyklus
- Untersuchung von Ausfallmodi und Wiederherstellungsprozessen
- Einführung eines standortübergreifenden Clustering
- Verstehen der Migrationsverfahren
- Übung 6: Index-Cluster aktualisieren
- Übung 7: Cluster erweitern und Indexer-Daten migrieren

Thema 9 - Clustering von Suchköpfen

- Überblick über das Search Head Clustering geben
- Erklären, wie man einen Cluster verwaltet und einsetzt
- Beschreibung der Inhaltsverwaltung mit dem Deployer
- Überprüfung der Rolle der Mitglieder des Clusters und des Kapitäns
- Labor 8 - SHC installieren

Anhang A - REST API

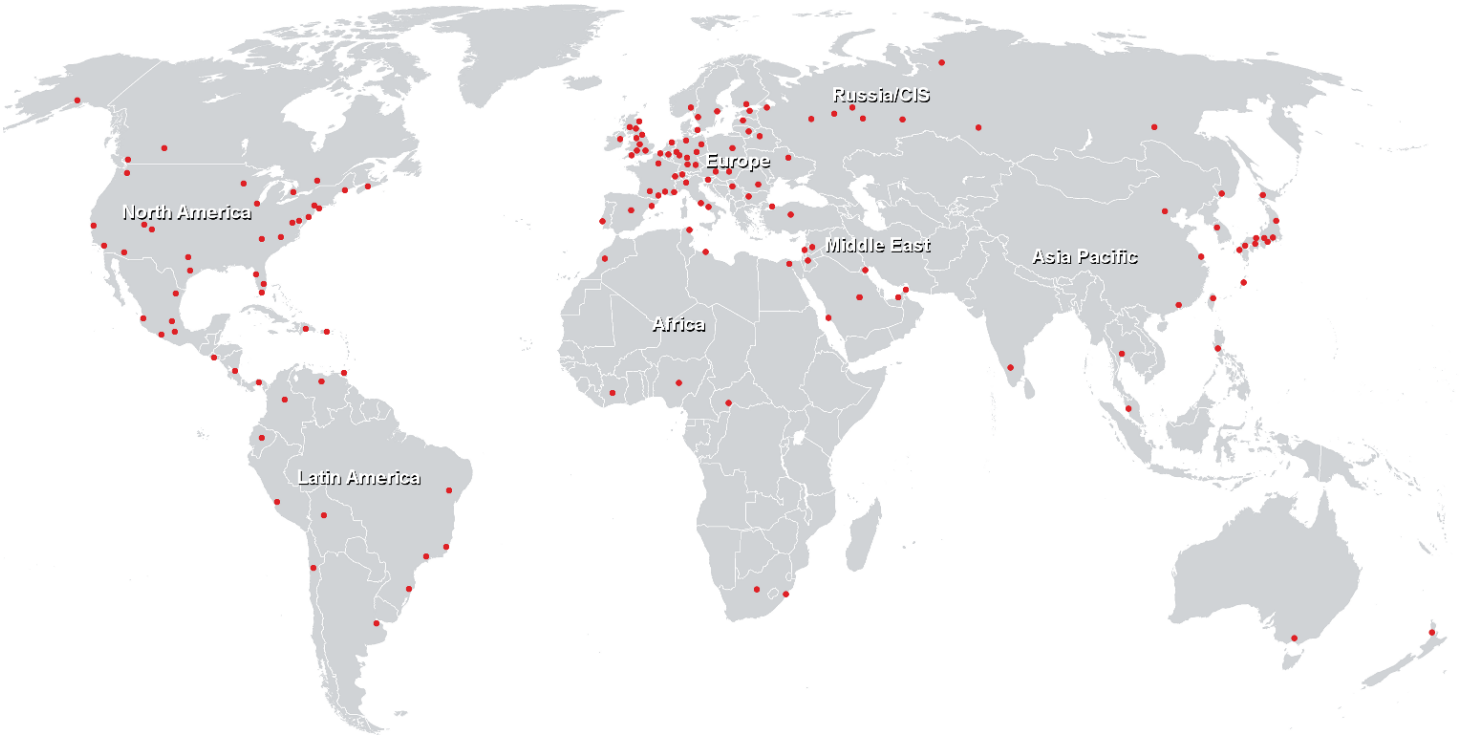
- Definieren Sie die Splunk REST API
- Erörterung von Anfragen, Endpunkten und Namespaces
- Untersuchung von Werkzeugen und Methoden zur Nutzung der API

Kursinhalt

- Splunk-Architektur
- Überwachungskonsole
- Bereitstellungsserver
- LDAP-Integration
- Sammeln und Weiterleiten von Daten
- Indizierung und Suche
- Clustering-Indexer
- Clustering von Suchköpfen

Services Core Implementation (SCI)

Weltweite Trainingscenter



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