Splunk - Architect Fast Start

Dieser Kurs konzentriert sich auf die Bereitstellung in großen Unternehmen.

Die Teilnehmer lernen:

• Schritte und Best Practices für die Planung, Datenerfassung und Dimensionierung eines verteilten Deployments.
Themen und Techniken zur Fehlerbehebung bei einer verteilten Standard-Splunk-Installation unter Verwendung der in Splunk Enterprise verfügbaren Tools.
• Erfahrungen bei der Fehlersuche vor der Teilnahme an fortgeschritteneren Kursen. Sie werden eine verteilte Splunk Enterprise-Umgebung mit Hilfe des Live-Systems debuggen.
• das grundlegende Wissen über die Bereitstellung und Verwaltung von Splunk Enterprise in einer Cluster-Umgebung. Es deckt die Installation, Konfiguration, Verwaltung und Überwachung von Splunk Clustern ab.

Während Splunk Cluster in Windows-Umgebungen unterstützt werden, laufen in der Kursumgebung nur Linux-Instanzen. NUR für Kunden mit Splunk on-prem.

Kursinhalt
• Architecting Splunk Enterprise Deployments:
• Introduction
• Project Requirements
• Infrastructure Planning: Index Design
• Infrastructure Planning: Resource Planning
• Clustering Overview
• Forwarder and Deployment Best Practices
• Integration
• Performance Monitoring and Tuning
• Use Cases
• Splunk Troubleshooting Methods and Tools
• Indexing Problems
• Input Configuration Problems
• Input Deployment Problems
• Indexer Cluster Management Administration
• License, Upgrade, and User Management Problems
• Search Management Problems
• KV Store Collection and Lookup Management
• Large-scale Splunk Deployment Overview
• Single-site Indexer Cluster
• Multisite Indexer Cluster
• Indexer Cluster Management and Administration
• Forwarder Management
• Search Head Cluster
• Search Head Cluster Management and Administration
• KV Store Collection and Lookup Management
• SmartStore Implementation

Voraussetzungen
Um erfolgreich zu sein, sollten die Studierenden ein solides Verständnis der folgenden Kurse haben:

• Splunk Power User Fast Start
• Splunk Enterprise Administration Fast Start

Kursziel
Splunk Enterprise Certified Architect (Vorausgesetzt für diese Zertifizierung werden der Splunk Core Certified Power User UND der Splunk Enterprise Certified Admin)

Dieser Kurs im Web
Alle tagesaktuellen Informationen und Möglichkeiten zur Bestellung finden Sie unter dem folgenden Link: www.experteach.de/go/**SKAR**

Vormerkung
Sie können auf unserer Website einen Platz kostenlos und unverbindlich für 7 Tage reservieren. Dies geht auch telefonisch unter 06074 4868-0.

Garantierte Kurstermine
Für Ihre Planungssicherheit bieten wir stets eine große Auswahl garantierter Kurstermine an.

Ihr Kurs maßgeschneidert
Diesen Kurs können wir für Ihr Projekt exakt an Ihre Anforderungen anpassen.

Training		**Preise zzgl. MwSt.**
Termine in Deutschland	**5 Tage**	**€ 4.000,-**
Online Training	**5 Tage**	**€ 4.000,-**
Termin/Kursort		Kurssprache Deutsch
28.07.-01.08.25 ONOnline		15.12.-19.12.25 ONOnline
08.09.-12.09.25 ONOnline		

Stand 07.05.2025

ExperTeach

Inhaltsverzeichnis

Splunk - Architect Fast Start

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 test environment performance
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

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 – Input Deployment Problems
Deployment server issues
Forwarding and Receiving Issues

Module 5 – Indexer Cluster Management Administration
Peer Offline and Decommission
Master App Bundles
Indexer Cluster Storage Utilization Options
Site Mapping
Monitoring Console for Indexer Cluster Environment

Module 6 – License, Upgrade, and User Management Problems
Installation Issues
Upgrade Considerations
Splunk Licensing Issues
Splunk Roles and User Management issues

Module 7 – Search 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 – KV Store Collection and Lookup Management
Identify the Types of Search Problems
Isolate and Troubleshoot Search Problems
Splunk Enterprise Cluster Administration :

Module 1 – Large-scale Splunk Deployment Overview
Factors that affecting deployment design
How Splunk Enterprise can scale
Splunk License Master

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 Multi-site Indexer Clusters Work
Multi-Site Indexer Cluster Terms
Multi-Site Indexer Cluster Configurations
Optional Multi-Site 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

Module 5 – Forwarder Management
Indexer discovery
Optional Indexer Discovery Configurations
Volume-Based Forwarder Load Balancing

Module 6 – Search Head Cluster
Splunk Search Head Cluster Overview
Search Head Cluster Configuration

Module 7 – Search Head Cluster Management and Administration
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 – SmartStore Implementation
SmartStore Architecture Overview
Deploy and manage SmartStore

ExperTeach Gesellschaft für Netzwerkkompetenz mbH
Waldstr. 94 · 63128 Dietzenbach · Telefon: +49 6074 4868-0 · Fax: +49 6074 4868-109 · info@experteach.de · www.experteach.de