



Enterprise Computing Solutions - Education Services

TRAINING OFFERING

Sie erreichen uns hier

Freistädterstraße 236, A-4040 Linz

Email: education.ecs.at@arrow.com

Phone: +43 1 370 94 40 - 34



Splunk Architect Fast Track

CODE:	LÄNGE:	PREIS:
SPL_ARCH-FT	40 Hours (5 Tage)	€4,000.00

Description

This course focuses on large enterprise deployments. Students will learn :

- steps and best practices for planning, data collection and sizing for a distributed deployment.
 - topics and techniques for troubleshooting a standard Splunk distributed deployment using the tools available on Splunk Enterprise.
 - troubleshooting experience before attending more advanced courses. You will debug a distributed Splunk Enterprise environment using the live system. case logs.
 - the fundamental knowledge of deploying and managing Splunk Enterprise in a clustered environment. It covers installation, configuration, management, and monitoring of Splunk clusters.
- While Splunk Clusters are supported in Windows environments, the class lab environment is running Linux instances only.
ONLY for customers with Splunk on-prem

Lernziel

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

SmartStore Architecture Overview

KV Store Monitoring with Monitoring Console Module 9 – SmartStore Implementation Deploy and manage SmartStore

Voraussetzungen

To be successful, students should have a solid understanding of the following courses: Splunk Power User Fast Start
Splunk Enterprise Administration Fast Start

Test und Zertifizierung

Splunk Enterprise Certified Architect (Prereq for this cert is the Splunk Core Certified Power User AND Splunk Enterprise Certified Admin)

Kurstermine

Auf Anfrage. Bitte [kontaktieren Sie uns](#)

Zusätzliche Information

[Diese Schulung ist auch als Vor-Ort-Schulung verfügbar. Bitte kontaktieren Sie uns, um mehr zu erfahren.](#)