ARROW

Enterprise Computing Solutions - Education Services

TRAINING OFFERING

Du kan nå os her

.

Email: training.ecs.dk@arrow.com
Phone: +45 7025 4500

splunk>   Splunk 9.0 Cluster Administration

CODE:	LENGTH:	PRICE:
SPL_SCLUA9	24 Hours (3 dage)	kr 11,190.00

Description

This 3-virtual day course is for an experienced Splunk Enterprise administrator who is new to Splunk Clusters. The course provides 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.

Objectives

- Large-scale Splunk Deployment Overview
- Single-site Indexer Cluster
- Indexer Cluster Management and Administration
- Forwarder Configuration
- Search Head Cluster
- Search Head Cluster Management and Administration
- KV Store Collection and Lookup Management
- SmartStore Implementation Overview

Prerequisites

To be successful, students should have a solid understanding of the following courses:

- Splunk Fundamentals 1

- Splunk Fundamentals 2

OR the following single-subject courses:

- What Is Splunk?

- Intro to Splunk

- Using Fields

- Scheduling Reports and Alerts

- Visualizations

- Leveraging Lookups and Subsearches

- Search Under the Hood

- Introduction to Knowledge Objects

- Creating Knowledge Objects

- Enriching Data with Lookups

- Data Models

- Introduction to Dashboards
  Students should also have completed the following courses:

- Splunk System Administration

- Splunk Data Administration

- Troubleshooting Splunk Enterprise

Programme

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

Session Dates

Date	Location	Time Zone	Language	Type	Guaranteed	PRICE
24 Apr 2024	Virtual Classroom (CET / UTC +1)	CEDT	English	Instructor Led Online		kr 11,190.00

Yderligere Information

Denne træning er også tilgængelig som træning på stedet. Kontakt os for at finde ud af mere.