SPLUNK TRAINING

# Splunk Enterprise Certified Admin Course

*Master Splunk Enterprise administration. Get certified to manage Splunk deployments and analyze machine data effectively.*

**DURATION**
**2 hours**

**LEVEL**
**Intermediate**

**FORMAT**
**Instructor-Led**

- Globally Recognized Certification
- Expert-Led Hands-On Training
- Flexible Scheduling

Computer Pride | 1st Floor, ICEA Building, Kenyatta Avenue, Nairobi | www.computer-pride.co.ke

## COURSE OVERVIEW

This intermediate-level Splunk Enterprise Certified Admin Course is meticulously designed for IT professionals aiming to master the administration, management, and troubleshooting of Splunk Enterprise environments. Over two intensive hours, participants will delve into the critical aspects of Splunk deployments, including data ingestion, indexer and search head cluster management, user and role-based access control, and performance optimization. The course emphasizes practical skills required to maintain robust, efficient, and secure Splunk instances.
Upon completion, you will possess the expertise to confidently manage Splunk operations, ensuring optimal data availability and system health. This certification not only validates your technical proficiency in administering Splunk Enterprise but also positions you as a valuable asset in organizations leveraging Splunk for operational intelligence, security monitoring, and business analytics. It empowers you to streamline IT operations, enhance security posture, and contribute significantly to data-driven decision-making processes.

| | |
|---|---|
| **Duration** | 2 hours |
| **Level** | Intermediate |
| **Vendor** | Splunk |

## COURSE CURRICULUM

### 01 Module 1: Splunk Enterprise Fundamentals & Architecture

- Review of Splunk Core Components (Indexer, Search Head, Forwarder, Deployment Server)
- Understanding Single-Instance vs. Distributed Deployments
- Splunk Licensing and System Requirements
- Installing and Configuring Splunk Enterprise

### 02 Module 2: Data Ingestion and Configuration

- Configuring Data Inputs (Files & Directories, Network Data, Scripts)
- Managing Forwarders (Universal and Heavy Forwarders)
- Using props.conf and transforms.conf for Data Parsing and Manipulation
- Monitoring Data Ingestion Health

### 03 Module 3: Index Management and Storage Optimization

- Creating and Managing Indexes
- Understanding Bucket Lifecycle and Data Retention Policies
- Strategies for Storage Optimization and Performance Tuning
- Troubleshooting Indexing Issues

### 04 Module 4: User Administration and Security

- Managing Users, Roles, and Capabilities
- Configuring Authentication Methods (LDAP, SAML, Native)
- Implementing Access Controls for Data and Features
- Securing Splunk Communications (SSL/TLS)

### 05 Module 5: Distributed Search and Cluster Management

- Configuring and Managing Search Head Clusters
- Understanding and Administering Indexer Clusters (Cluster Master, Peer Nodes)
- Deployment Server for Centralized Configuration Management
- Best Practices for Scaling Splunk Deployments

### 06 Module 6: Monitoring, Troubleshooting, and Maintenance

- Monitoring Splunk System Health (DMC, internal logs)
- Troubleshooting Common Splunk Issues (Performance, Data Gaps)
- Backup and Recovery Strategies
- Splunk Maintenance Tasks and Upgrades

## CAREER PATHWAYS

Graduates of this program are prepared for the following roles:

> **Splunk Administrator**

> **Security Operations Center (SOC) Engineer specializing in Splunk**

> **IT Operations & Monitoring Specialist with Splunk Expertise**

## FREQUENTLY ASKED QUESTIONS

**Q: What specific challenges does a Splunk Enterprise Certified Admin solve in a typical enterprise environment?**

A Splunk Enterprise Certified Admin is equipped to tackle critical challenges such as ensuring continuous data ingestion from diverse sources, optimizing indexer performance to handle large data volumes, managing user access securely across departments, and maintaining high availability of Splunk search environments. They are key in troubleshooting data parsing issues, resolving performance bottlenecks, and implementing scalable Splunk architectures that support operational intelligence and security monitoring needs.

**Q: What are the recommended prerequisite skills or knowledge for enrolling in the Splunk Enterprise Certified Admin Course?**

While this is an intermediate-level course, it is highly recommended that participants have a foundational understanding of Splunk search concepts, equivalent to completing the Splunk Core Certified User certification or having practical experience with Splunk searches and dashboards. Familiarity with Linux command-line interface, networking basics, and general IT administration principles will also be beneficial for grasping the advanced administration topics covered.

**Q: How does this certification specifically enhance my ability to manage a large-scale Splunk deployment with multiple data sources?**

This certification focuses heavily on the architecture and management of distributed Splunk environments, including search head clusters and indexer clusters. You will learn to configure and manage data ingestion from hundreds of sources using forwarders, optimize indexer performance for massive data volumes, and implement robust deployment strategies using the deployment server. The curriculum explicitly covers scaling best practices and troubleshooting techniques essential for maintaining complex, high-volume Splunk deployments, making you proficient in handling enterprise-level data processing and analysis needs.

## ABOUT COMPUTER PRIDE

computerpride

*East Africa's Premier IT Training Center*

With over 15 years of excellence, Computer Pride delivers globally recognized certification programs from leading technology vendors. Located on Kenyatta Avenue in Nairobi's CBD, our state-of-the-art facilities and expert instructors have empowered thousands of professionals across East Africa.

| 15+ | 10,000+ | 50+ |
|---|---|---|
| Years of Excellence | Professionals Trained | Vendor Certifications |

## READY TO ENROL?

Take the next step in your technology career.

**Location**
1st Flr, ICEA Building
Kenyatta Ave, Nairobi

**Email**
info@computer-pride.co.ke

**Phone**
+254 705 900 900

**www.computer-pride.co.ke**