

---

At EDUCBA, it is a matter of pride to us to make job oriented hands on courses available to anyone, any time and anywhere.

Learn at a time and place, and pace that is of your choice.

Plan your study to suit your convenience and schedule.

# SPLUNK TRAINING

---

Email Contact: [info@educba.com](mailto:info@educba.com)



# EDUCBA

---



[www.educba.com](http://www.educba.com)

# Course Overview

---

This Splunk certification is mainly for software developers who wish to implement Splunk in operational intelligence of machine data.

Basic fundamentals of Splunk is where you learn to correlate events, dynamic searching, workflows. This Splunk training helps to use Splunk in Application Management, Business Analytics.

# Splunk Training Skills

---

Through this course you will be familiar with implementing Splunk in the current workplace for indexing, mapping knowledge, alerts, creating interactive dashboards, searching, visualizations to focus on growth.

You can efficiently build web framework using web technologies skills like for client-side Splunk javascript component is deployed similarly for server-side it supports Python.

# Course Features

---



Course Duration-  
56+ Hours



Number of Courses



Verifiable  
Certificates



Lifetime Access



Technical  
Excellence

# About Splunk

---

Splunk is a versatile software analytical tool used for searching, analyzing real-time machine-generated big data. It is originated as a search engine for the log files stored in the infrastructure.

It works with huge volumes of data to analyze machine-generated outputs and resolve data analytics problems with any size.

Splunk can be defined as pulling data from Multiple systems and data sets using keys and indexer in real time and turn machine data.

# Splunk Course

---

This is a Bundle Course that includes complete in-depth Splunk Learning Courses combined into one Complete Course.

This Bundle perfectly meets the requisite of the industry and gives you a better chance of being hired as a Splunk professional.

# 1

# Splunk Fundamentals

---

## Section 1. Introduction

- Introduction to Splunk

## Section 2. Intelligence and Example

- Operational Intelligence
- Splunk Examples

## Section 3. Splunk MapReduce

- Splunk MapReduce

## Section 4. Installation

- Splunk Enterprise Windows Installation
- Splunk Enterprise Setup

## Section 5. Basic configurations

- Basic Configurations of Splunk

## Section 6. Data Input into Splunk

- Data Input into Splunk

## Section 7. Splunk Apps and Searching the data

- Introduction to Splunk Apps
- User Interface of Splunk
- Searching the data in Splunk
- Fields Side Bar
- Format Timeline

## Section 8. Splunk Fields, Splunk Searching and Reporting App Tour

- Splunk Fields
- Splunk Searching
- Reporting App Tour

## Section 9. Splunk Report Creation

- Splunk Report Creation

## Section 10. Splunk statistics and visualization

- Splunk Statistics
- Splunk Visualization

# 1

# Splunk Fundamentals

---

## Section 11. Splunk Search Commands

- Splunk Search Commands
- Rename Command
- Search Fundamentals
- Remove Duplicates and Sort

## Section 12. Splunk Commands

- Splunk Commands Top Rare

## Section 13. Deriving statistics

- Stats Command
- Count Function in Stats
- Distinct Count Function in Stats
- Sum and Average Function in Stats
- List and Value Function in Stats

## Section 14. Creating Visualizations

- Splunk Chart Command
- About Time Chart in Splunk
- Splunk Charts Line Area
- Line chart in Splunk Using Chart and Time Chart
- Area Chart in Splunk using Chart and Time Chart
- Bar Chart in Splunk
- Pie chart in Splunk
- Bubble and Scatter chart Visualizations in Splunk
- Single and Gauges type visualizations in Splunk

## Section 15. Enriching Visualizations

- Splunk Single Value Visualizations
- Add Totals and uses of Add Totals in Splunk
- Splunk Trend Line Command
- Cluster Map Visualization



# Splunk Fundamentals

---

## Section 16. Evaluating the Results

- Splunk using Eval Command
- Splunk Stats Eval
- Splunk ToString Function
- Splunk if Function
- Splunk Filtering Results

## Section 17. Correlating Events

- Splunk Transaction Command
- Splunk Transaction Maxspan and Maxpause  
starts with Ends with
- Correlating Events

# 2

## Splunk Advanced 01 – Knowledge Objects

---

### Section 1. Introduction

- Introduction Splunk Knowledge Objects

### Section 2. Splunk CIM and Permissions

- Command Information Models in Splunk
- Splunk Permissions Options

### Section 3. Splunk Lookups

- Splunk Lookups
- How to Define a Lookups
- Lookups Commands in Splunk
- Automatic Lookups in Splunks
- Time Based Lookups
- Splunk Field Aliases
- Splunk Calculated Fields

### Section 4. Splunk Lookups

- Introduction Splunk Field Extractions
- Field Extraction Regex Settings in Splunk
- Splunk Field Extraction Regex Sidebar
- Splunk Field Extraction Regex Event Actions
- Splunk Field Extractions Delimiters Settings Menu
- Splunk Field Extractions Delimiters Fields Sidebar
- Splunk Field Extractions Delimiters Event Actions

# 2

## Splunk Advanced 01 – Knowledge Objects

### Section 5. Splunk Workflow Actions

- Splunk Workflow Actions GET
- Splunk Workflow Actions POST
- How to Create Post Action
- Splunk workflow Actions Search
- Example Splunk Workflow Actions Search

### Section 6. Splunk Tags

- How to Create a Tag in Splunk
- How to Use a Tag in Splunk
- Unique Tag Object

### Section 7. Splunk Event Types

- How to Create Event type
- Highlight Event Type Using Colors
- Patterns Tab

### Section 8. Splunk Alerts

- Splunk Alerts
- Triggers Conditions Splunk
- Triggers Action Alerts
- Alerts using Patterns Tab

### Section 9. Splunk Scheduled Reports

- Splunk Scheduled Reports
- Editing the Scheduled Reports

### Section 10. Managing Splunk Scheduled Reports

- Managing Splunk Scheduled Reports

### Section 11. Splunk Report Dashboards

- Creating a Splunk Dashboard
- Formats of Dashboard
- HTML Dashboard



# 2

## Splunk Advanced 01 – Knowledge Objects

---

### Section 12. Splunk Macros

- Splunk Macros
- Splunk Macros with Arguments
- Managing Splunk Macros

### Section 13. Splunk Data Models/Pivots

- Splunk Data Models
- Attribute in Splunk Data Model
- Attribute Flags Splunk Data Model
- Look ups with Data Model
- Splunk Data Model Hierarchy
- Splunk Transaction Objects
- Splunk Data Models Uploading Downloading
- Splunk Data Models Acceleration
- Creating Splunk Pivots
- Line chart Visualization in Pivaot
- Area Chart and Bar Graph Visualization
- Creating Instant Pivot

# 3

## Splunk Advanced Administration 02 –

### Section 1. Introduction

- Introduction to Splunk Component

### Section 2. Splunk Components

- Search Head and Forwarder Components in Splunk
- Deployment Server and License Master

### Section 3. Splunk Hardware Components

- Hardware Requirement for Splunk

### Section 4. Splunk directory structure

- Splunk Directory Structure

### Section 5. Splunk Conf Files and Splunk Indexes

- Splunk Configuration File
- Props Configuration and Transom Configuration

### Section 6. Splunk Access Controls Overview

- Splunk Access Controls Overview
- Example of Splunk Access Control

### Section 7. Growth of Splunk Deployments

- Splunk Distributed Environment
- Search Peer Example in Splunk

### Section 8. Splunk Instance

- Single Instance Deployment in Splunks
- Multi Instance Deployment in Splunks
- OS Permissions in Splunk
- Splunk D Process and Splunk Port
- Splunk Pipeline and Its Segments

## Section 9. Splunk Licensing

- Splunk Licensing
- License and Warning in Splunks

## Section 10. Splunk Indexes

- Splunk Indexes
- Default Indexes in Splunks

## Section 11. Using Multiple Indexes

- Web Data Index In Splunk
- Security index in Splunk

## Section 12. Splunk Index Buckets

- Splunk Index Buckets
- Hot Splunk Index Buckets
- Warm Splunk Index Buckets

## Section 13. Configuration Files

- Splunk Configuration Files
- Splunk Configuration Files Example
- Splunk Configuration Directories
- Flowchart of Configuration Directories
- Splunk Index time
- Splunk Search time
- No Conflicts Splunk Config File Merge
- No Conflicts Splunk Config File Merge Flowchart
- Splunk Config File Merge Conflicts
- Example of Merge Conflicts
- Splunk Btool Command
- Splunk of Btool Command Example

### Section 14. Splunk Index

- Splunk Index Management
- Types of Index Management in Splunk
- Creation of Splunk Indexes
- Splunk Index Size Estimates
- Splunk Index Integrity Check
- How to Configure a Splunk File
- Additional Settings in Splunk Configure File
- Example in Splunk Configure File
- Splunk Retention Policy
- Types of Splunk Retention Policy
- Strict Volume Base Retention Policy

### Section 15. Splunk Users

- Splunk Access Controls

### Section 16. Splunk Roles

- Splunk Default Roles
- Creation of Splunk Roles
- Example of Splunk Roles
- Splunk Access Controlsof Default Indexes
- Splunk Access Controls on Indexes
- Splunk Role Inheritance
- Methods of Role Inheritance
- Splunk Role Capabilities

### Section 17. Splunk Authentication

- Splunk Users Role
- Splunk Native Authentication Access Control
- Splunk Admin Access Control
- Working with LDAP Authentication Optio
- Flowchart of LDAP Authentication
- How to Configure a LDAP Server
- Exampler of LDAP Server
- Working Sampl in using LDAP Server
- How to Configure a SAMPL Server
- Single Sign out with Reverse Proxy
- Splunk Scripted Authentication

### Section 18. Splunk Universal Forwarders

- Splunk Universal Forwarders
- Installation of Universal Forwarder
- Downloading Universal Forwarder
- Validating Forwarder Installation
- Checking Management Port
- Splunk Status Command
- Configuration of Splunk Universal
- Configuring Listening Port
- Indexer File
- Testing the Connection
- Troubleshoot the Connection
- Securing The Data Feed
- Automatic Load Balancing

### Section 19. Splunk Forwarder Management

- Recap on Advanced Forwarder
- Configuration of Forwarder Inputs
- Forwarding Monitoring and Management
- Forwarder Asset Table
- Splunk Forwarder Management
- Compressing Data Feed
- Connection through Data Manager
- Components of Deployment Server
- Creating Folder in Linux
- Overview on Deployment Server
- Forwarder Management
- Creating Deployment App
- Configuring Deployment App

### Section 20. Data Inputs in Splunk

- Splunk Index Time Process
- Understanding the Monitor
- Selecting the Checkpoints
- Setting Source Type
- Describing Host Field
- Forward Option
- Monitoring Consoe

### Section 21. Monitoring Data Inputs in Splunk

- Monitor Inputs
- Multi Line Log Files
- Input Settings
- Monitoring Inputs
- Settings with Host Field
- Monitoring Directory
- Files and Directories
- Monitor Line for Source File
- Segments of Wildcards
- Dot Log Files
- Advanced Options for Input File
- Blacklist Precedence

### Section 22. Splunk Universal Forwarders

- Configuring the Data Forwarding
- Data Feed Advantages and Disadvantages
- Forwarder and Receiving Index

### Section 23. Network Inputs

- Difference in queue
- Persistent Queue
- Scripted Inputs
- Creating a Script
- Processing on Scripting Inputs
- Scheduling per Requirement
- Data Inputs

### Section 24. Windows and Agentless inputs

- Windows Inputs and Agentless Inputs
- Windows Specific Inputs
- Types of Windows Specific Inputs
- Settings for App Context
- Local Performance Monitor
- Settings in Input Files
- Event Log Monitoring
- Powershell Inputs
- Splunk Agentless Inputs
- HTTP event collector
- Specifying Metadata

## Section 25. Fine-Tuning Splunk inputs

- Fine Tuning Inputs
- Props Dot Conf
- Data Modifications in Props
- Creating Monitor Input
- Parsing Phase and Data Preview
- Event Boundaries
- Single Line Source Type
- Setting Time Zone
- Multi Line Events
- Date and Time Stamp
- Data Preview Screen
- Time Stamp Field
- Method of Classification

## Section 26. Manipulating Raw Data

- Manipulating Raw Data
- Using the Regex
- Event Based Transformation
- Log File for Regex
- Understanding Regex
- Indexing the Log File
- Setting up Host names

## Section 27. Supporting KO's

- KV Based lookups
- Types of Lookups

## Section 28. Data Access Risks

- Mitigating Possible Data Access Risks
- The Available Capabilities in Splunk
- Restricting Unauthorized Users in Splunk

## Section 29. Distributed Search Authentication

- Learning about the Distributed Search
- Understanding the Distributed Architecture
- Standalone and Distributed Architecture
- Setting up Distributed Search
- Differences in Clustered and Non Clustered Indexers
- Distributed Search Authentication
- Best Practices using Distributed Search
- Understanding the Dedicated Search Heads
- Determining the Search Head Cluster

## Section 30. Performance Tuning

- Performance Tuning in Splunk
- Splunk Data Pipelines
- Setting the Index Parallelization
- Index Storage Optimization
- Concept of Search Performance
- Reports Designed in Splunk
- Schedule Window in Search Performance
- Managing the Search Jobs
- Runtime to Search the Query
- Evaluating on the Saved Option
- Using the Search Parallelization
- Learning the Real Time Search


## Section 31. Problem Isolation

- Log Levels in Splunk
- Types of Splunk Log Levels
- Modifying the Splunk Level
- Functions of Indexing Processes
- Running the Splunk Diag Command

## Section 32. Large Scale Deployments

- Large Scale Splunk Deployment





# Frequently Asked Questions

---

Why this Splunk Training is demanded more?

As we all know that a machine data is being generated in a fast manner and the companies are looking forward to parsing this Big data and converting them into business importance, that's why this training is demanded more.

What are the benefits of becoming a Splunk Professional?

Being Splunk Professional, we can help an organization to understand the customer's requirements, behaviour. You can fetch relevant information from the waste of data (unstructured data). As a splunk admin, you get the compete for highest paying IT jobs.

What are the course outcomes in Splunk certification?

This Splunk training is more suitable for the candidates who want to shine themselves in Machine learning, System Administrators. You have a flourishing career in the cloud and big data environment.



# Customer Reviews

“

This is an excellent course. I am really obtaining good knowledge and I am sure that I will use it in my daily activities. The instructor language is clear and concise. He demonstrates various concepts and explains the results as he goes along. There was some useful information and it was presented in a proper order.

AHMAD MOHAMMAD

”

I strongly recommend this Splunk training certification to my colleagues who are interested in making their path in data analytics as they are the one of the most top log Analytics availing in the current market. You will also learn to find correlations of data depends on time, location and other factors. the core components of splunk for implementations are explained in a good manner.

Dophin Fernandez



**EDUCBA**

---

# Splunk Training Course

---

For Queries please contact:

Email : [info@educba.com](mailto:info@educba.com)



[www.educba.com](http://www.educba.com)