About Intellipaat

Intellipaat is a global online professional training provider. We are offering some of the most updated, industry-designed certification training programs in the domains of Big Data, Data Science & AI, Business Intelligence, Cloud, Blockchain, Database, Programming, Testing, SAP and 150 more technologies.

We help professionals make the right career decisions, choose the trainers with over a decade of industry experience, provide extensive hands-on projects, rigorously evaluate learner progress and offer industry-recognized certifications. We also assist corporate clients to upskill their workforce and keep them in sync with the changing technology and digital landscape.

About The Course

This is an Intellipaat masters' program in Splunk tool that includes Splunk developer and Splunk administration training. As part of this Splunk course, you will work on searching, sharing, saving Splunk results, creating tags, generating reports and charts, installing and configuring Splunk, monitoring, scaling and indexing large volumes of searches and analyzing it using the Splunk tool.

Why take this Course?

Splunk is the most popular tool used for parsing huge volumes of machine-generated data and deriving valuable insights from it. This Intellipaat instructor-led and self-paced training in Splunk Developer and Splunk Administration is your passport to working in the Splunk domain in order to gain a definitive edge when it comes to deploying Splunk in mission-critical applications in the real world in top MNCs and commanding big salaries in the process.

Course Content

Splunk Developer

1. Splunk Development Concepts
2. Basic Searching
3. Using Fields in Searches
4. Saving and Scheduling Searches
5. Creating Alerts
6. Scheduled Reports
7. Tags and Event Types
8. Creating and Using Macros
9. Workflow
10. Splunk Search Commands
11. Transforming Commands
12. Reporting Commands
13. Mapping and Single Value Commands
14. Splunk Reports and Visualizations
15. Analyzing, Calculating and Formatting Results
16. Correlating Events
17. Enriching Data with Lookups
18. Creating Reports and Dashboards
19. Getting Started with Parsing
20. Using Pivot
21. Common Information Model (CIM) Add-On

Splunk Administration

1. Overview of Splunk
2. Splunk Installation
3. Splunk Installation in Linux
4. Distributed Management Console
5. Introduction to Splunk App
6. Splunk Indexes and Users
7. Splunk Configuration Files
8. Splunk Deployment Management
9. Splunk Indexes
10. User Roles and Authentication
11. Splunk Administration Environment
12. Basic Production Environment
13. Splunk Search Engine
14. Various Splunk Input Methods
15. Splunk User and Index Management
16. Machine Data Parsing
17. Search Scaling and Monitoring
18. Splunk Cluster Implementation

Splunk Development Concepts

- Introduction to Splunk and Splunk developer roles and responsibilities

Basic Searching

- Writing Splunk query for search
- Auto-complete to build a search, time range, refine search, working with events
- Identifying the contents of search and controlling a search job

Using Fields in Searches

- What is a Field and how to use Fields in search
- Deploying Fields Sidebar and Field Extractor for REGEX field extraction and delimiting Field Extraction using FX

Saving and Scheduling Searches

- Writing Splunk query for search, sharing, saving, scheduling and exporting search results

Creating Alerts

- How to create alerts, understanding alerts and viewing fired alerts.

Scheduled Reports

- Describe and configure scheduled reports

Tags and Event Types

- Introduction to Tags in Splunk
- Deploying Tags for Splunk search
- Understanding event types and utility and generating and implementing event types in search

Creating and Using Macros

- What is a Macro and what are variables and arguments in Macros

Workflow

- Creating get, post and search workflow actions

Splunk Search Commands

- Studying the search command and the general search practices
- What is a search pipeline
- How to specify indexes in search
- Highlighting the syntax and deploying the various search commands like fields, tables, sort, rename, rex and erex

Transforming Commands

- Using top, rare and stats commands

Reporting Commands

- Using following commands and their functions: addcoltotals, addtotals,top, rare and stats

Mapping and Single Value Commands

- IPlocation, geostats, geom and addtotals commands

Splunk Reports and Visualizations

- Explore the available visualizations
- Create charts and time charts
- Omit null values and format results

Analyzing, Calculating and Formatting Results

- Calculating and analyzing results

- Value conversion, roundoff and format values
- Using the eval command
- Conditional statements and filtering calculated search results

Correlating Events

- How to search the transactions
- Creating report on transactions
- Grouping events using time and fields and comparing transactions with stats

Enriching Data with Lookups

- Learning data lookups
- Examples and lookup tables
- Defining and configuring automatic lookups and deploying lookups in reports and searches

Creating Reports and Dashboards

- Creating search charts, reports and dashboards
- Editing reports and dashboards and adding reports to dashboards

Getting Started with Parsing

- Working with raw data for data extraction, transformation, parsing and preview

Using Pivot

- Describe pivot
- Relationship between data model and pivot
- Select a data model object
- Create a pivot report
- Create in stant pivot from a search and add a pivot report to dashboard

Common Information Model (CIM) Add-On

- What is a Splunk CIM and using the CIM Add-On to normalize data

Overview of Splunk

- Introduction to the architecture of Splunk
- Various server settings, how to set up alerts
- Various types of licenses
- Important features of Splunk tool
- The requirements of hardware and conditions needed for installation of Splunk

Splunk Installation

- How to install and configure Splunk
- The creation of index
- Standalone server's input configuration
- The preferences for search
- Linux environment Splunk installation and the administering and architecting of Splunk

Splunk Installation in Linux

- How to install Splunk in the Linux environment
- The conditions needed for Splunk and configuring Splunk in the Linux environment

Distributed Management Console

- Introducing Splunk distributed management console
- Indexing of clusters
- How to deploy distributed search in Splunk environment
- Forwarder management, user authentication and access control

Introduction to Splunk App

- Introduction to the Splunk app
- How to develop Splunk apps, Splunk app management, Splunk app add-ons
- Using Splunk-base for installation and deletion of apps
- Different app permissions and implementation and how to use the Splunk app and apps on forwarder

Splunk Indexes and Users

- Details of the index time configuration file and the search time configuration file

Splunk Configuration Files

- Understanding of Index time and search time configuration filesin Splunk
- Forwarder installation
- Input and output configuration
- Universal Forwarder management and Splunk Universal Forwarder highlights

Splunk Deployment Management

- Implementing the Splunk tool
- Deploying it on the server
- Splunk environment setup and Splunk client group deployment

Splunk Indexes

- Understanding the Splunk Indexes
- The default Splunk Indexes
- Segregating the Splunk Indexes
- Learning Splunk Buckets and Bucket Classification
- Estimating Index storage and creating new Index

User Roles and Authentication

- Understanding the concept of role inheritance
- Splunk authentications, native authentications and LDAP authentications

Splunk Administration Environment

- Splunk installation, configuration
- Data inputs
- App management
- Splunk important concepts
- Parsing machine-generated data
- Search indexer and forwarder

Basic Production Environment

- Introduction to Splunk Configuration Files
- Universal Forwarder, Forwarder Management, data management, troubleshooting and monitoring

Splunk Search Engine

- Converting machine-generated data into operational intelligence
- Setting up the dashboard, reports and charts and integrating Search Head Clustering and Indexer Clustering

Various Splunk Input Methods

- Understanding the input methods
- Deploying scripted, Windows and network and agentless input types and fine-tuning them all

Splunk User and Index Management

- Splunk user authentication and job role assignment and learning to manage, monitor and optimize Splunk Indexes

Machine Data Parsing

- Understanding parsing of machine-generated data
- Manipulation of raw data
- Previewing and parsing
- Data field extraction and comparing single-line and multi-line events

Search Scaling and Monitoring

- Distributed search concepts
- Improving search performance
- Large-scale deployment and overcoming execution hurdles and working with Splunk Distributed Management Console for monitoring the entire operation

Splunk Cluster Implementation

- Cluster indexing
- Configuring individual nodes
- Configuring the cluster behavior, index and search behavior
- Setting node type to handle different aspects of cluster like master node, peer node and search head

Project Works

Project 1 : Creating an Employee Database of a Company

Industry : General

Problem Statement : How to build a Splunk dashboard where employee details are readily available

Topics : In this project, you will create a text file of employee data with details like full name, salary, designation, ID and so on. You will index the data based on various parameters, use various Splunk commands for evaluating and extracting the information. Finally, you will create a dashboard and add various reports to it.

Highlights :

- ✓ Splunk search and index commands
- ✓ Extracting field in search and saving results
- ✓ Editing event types and adding tags

Project 2 : – Building an Organizational Dashboard with Splunk

Industry : E-commerce

Problem Statement : How to analyze website traffic and gather insights

Topics : In this project, you will build an analytics dashboard for a website and create alerts for various conditions. You will capture access logs of the web server and the sample logs and then the sample are uploaded. You will analyze the top ten users, the average time spent, peak response time of the website, the top ten errors and error code description. You will also create a Splunk dashboard for reporting and analyzing.

Highlights :

- ✓ Creating bar and line charts
- ✓ Sending alerts for various conditions
- ✓ Providing admin rights for dashboard

Project 3 :– Field Extraction in Splunk

Industry : General

Problem Statement : How to extract the fields from event data in Splunk

Topics : In this project, you will learn to extract fields from events using the Splunk field extraction technique. You will gain knowledge in the basics of field extractions, understand the use of the field extractor, the field extraction page in Splunk web and field extract configuration in files. You will learn the regular expression and delimiters method of field extraction. Upon the completion of the project, you will gain expertise in building Splunk dashboard and use the extracted fields data in it to create rich visualizations in an enterprise setup.

Highlights :

- ✓ Field extraction using delimiter method
- ✓ Delimit field extracts using FX
- ✓ Extracting fields with the search command

Job Assistance Program

Intellipaat is offering job assistance to all the learners who have completed the training. You should get a minimum of 60% marks in the qualifying exam to avail job assistance.

Intellipaat has exclusive tie-ups with over 80 MNCs for placements.

Successfully finish the training | Get your resume updated | Start receiving interview calls

Intellipaat Alumni Working in Top Companies

Rahul Singh

Splunk Developer at Mindfire Solutions

This Intellipaat Splunk Training and Certification course is all you will need to work as a machine-data analyst who analyses machine-generated data to convert it into operational intelligence.

Chandra Sekhar Merugu

Senior System Engineer

Thanks to the entire Intellipaat team for quick response. I am more than happy to rank your service a 10 out of 10. You made it really worthwhile for me.

Arpita Khandelwal

Senior Threat Analysis Engineer at Hexaware Technologies

First, let me thank Intellipaat for having created such a wonderful Splunk online training course. The level of attention to detail and the manner in which the complex concepts have been explained in the Splunk course materials are praise worthy.

More Customer Reviews

Our Clients

+80 Corporates

Frequently Asked Questions

Q 1. What is the criterion for availing the Intellipaat job assistance program?

Ans. All Intellipaat learners who have successfully completed the training post April 2017 are directly eligible for the Intellipaat job assistance program.

Q 2. Which are the companies that I can get placed in?

Ans. We have exclusive tie-ups with MNCs like Ericsson, Cisco, Cognizant, Sony, Mu Sigma, Saint-Gobain, Standard Chartered, TCS, Genpact, Hexaware, and more. So you have the opportunity to get placed in these top global companies.

Q 3. Do I need to have prior industry experience for getting an interview call?

Ans. There is no need to have any prior industry experience for getting an interview call. In fact, the successful completion of the Intellipaat certification training is equivalent to six months of industry experience. This is definitely an added advantage when you are attending an interview.

Q 4. If I don't get a job in the first attempt, can I get another chance?

Ans. Definitely, yes. Your resume will be in our database and we will circulate it to our MNC partners until you get a job. So there is no upper limit to the number of job interviews you can attend.

Q 5. Does Intellipaat guarantee a job through its job assistance program?

Ans. Intellipaat does not guarantee any job through the job assistance program. However, we will definitely offer you full assistance by circulating your resume among our affiliate partners.