Splunk Administration

Course Summary

Description

The “Splunk Administration” course is targeted for administrators, architects, and software developers. After completing this course, students will learn how to successfully deploy Splunk using best practices. The course will also cover concepts for managing licenses, user and roles, and advanced topics like indexer and search head clustering. This course contains 10 labs for users to practice concepts they have learned during the course.

Topics

- Index Management
- User and Roles
- Forwarder Types and Management
- Configuration Files
- Apps
- Data Inputs
- Event Parsing
- Splunk Deployment Overview
- License Management
- Distributed Search
- Introduction to Splunk Clusters

Audience

The “Splunk Administration” course is targeted for administrators, architects, and software developers.

Prerequisites

- Splunk User Course
- Splunk Advanced User Course

Duration

Three days

Splunk Administration

Course Outline

I. ***Index Management***

A. Describe the role of the Splunk indexer, how indexes work, buckets and their lifecycle.
B. How to use Splunk Web, CLI, or indexes.conf to configure indexes
C. Describe how to configure indexes with using volumes
D. Reasons for having multiple indexes

II. ***User and Roles***

A. Review different roles and their capabilities available in Splunk
B. Walkthrough an example for creating a new user and assign a role

III. ***Forwarder Types and Management***

A. Review the differences between Universal and heavy forwarder
B. Overview on Forwarder Management/Deployment Server to manage forwarders and deployment clients

IV. ***Configuration Files***

A. Describe different configuration used in Splunk and their purpose:
   1. indexes.conf
   2. inputs.conf
   3. props.conf
   4. tranforms.conf
   5. web.conf
   6. serverclass.conf
B. Review configuration file structure
C. Review configuration file priority/ precedence

V. ***Apps***

A. Review apps for packaging configurations, views, lookups
B. The difference between Apps vs addons
C. Review app directory structure
D. How to Install an app via Splunk Web and CLI, and command line
E. Review available options for managing apps including edit app permissions, disable an enable apps, and edit app properties
F. Review Premium developed by Splunk to solve common data use cases. Apps include: Splunk Enterprise Security, Splunk ITSI, Splunk Behavior Analytics

VI. ***Data Inputs***

A. Describe different types of inputs:
   1. Files and directories
   2. Network inputs
   3. Scripted inputs
   4. Windows inputs
   5. Monitor inputs
B. Describe different methods for setting up data inputs with with apps, Splunk Web, command line interface, inputs.conf

VII. ***Event Parsing***

A. Describe how Splunk indexes data and how data moves from input to indexing phase.
B. Review configuration files involved in each phase of data pipeline

VIII. ***Splunk Deployment Overview***

A. Describe the role of indexer, forwarder, search head, deployment server in a Splunk deployment.
B. Review common Splunk deployment architectures
C. Review steps for downloading, installing, and starting Splunk.
D. Port management and common port numbers used in a Splunk deployment
E. Learn how to use the Monitoring Console to examine your Splunk environment. Describe different views available on the MC including views for search head and indexer cluster, forwarders, indexes and volumes, topology, health check.

Splunk Administration

Course Outline (cont.)

IX. ***License Management***

A. Review the different types of licenses in Splunk
B. Discuss how license warnings and violations work in Splunk
C. Managing Licenses
D. How to install a new license

X. Distributed Search

A. Understanding distributed search
   1. Search Head
   2. Forwarder
   3. Indexers

XI. ***Introduction to Splunk Clusters***

A. Introduce high availability into your deployment with indexer and search head clustering
B. Review concepts for indexer clustering including
C. Review concepts for search head clustering including