TechyEdz Solutions

Training | Consulting | Developement | Outsourcing

Server and Virtualization Monitoring
Infrastructure Monitoring
Application
Application Lifecycle and Release Analytics
splunk>
Event Management
Events Analytics
DevOps
Container Monitoring
Analytics
Predictive Analytics

Splunk Admin, Development & SIEM

☎ 9032803832

9032803832

contact@techyedz.com

www.techyedz.com

Splunk Admin, Development & SIEM Certification Training

- **Course Overview:**

This course is designed for system administrators who are responsible for managing the Splunk Enterprise environment. The Splunk Enterprise System Administration course focuses on administrators who manage a Splunk Enterprise environment. Topics include Splunk license manager, indexers and search heads, configuration, management, and monitoring. The Splunk Enterprise Data Administration course targets administrators who are responsible for getting data into Splunk.

- **Course Outline:**

Splunk Admin

Splunk Admin Basics

- Identify Splunk components

License Management

- Identify license types
- Understand license violations

Splunk Configuration Files

- Describe Splunk configuration directory structure
- Understand configuration layering
- Understand configuration precedence
- Use btool to examine configuration settings

Splunk Indexes

- Describe index structure
- List types of index buckets
- Check index data integrity
- Describe indexes.conf options
- Describe the fishbucket
- Apply a data retention policy

Splunk User Management

- Describe user roles in Splunk
- Create a custom role
- Add Splunk users

Splunk Authentication Management

- Integrate Splunk with LDAP
- List other user authentication options
- Describe the steps to enable Multifactor Authentication in Splunk

Getting Data In

- Describe the basic settings for an input
- List Splunk forwarder types
- Configure the forwarder
- Add an input to UF using CLI

Distributed Search

- Describe how distributed search works
- Explain the roles of the search head and search peers
- Configure a distributed search group
- List search head scaling options

Getting Data In – Staging

- List the three phases of the Splunk Indexing process
- List Splunk input options

Configuring Forwarders

- Configure Forwarders
- Identify additional Forwarder options

Forwarder Management

- Explain the use of Deployment Management
- Describe Splunk Deployment Server

- Manage forwarders using deployment apps
- Configure deployment clients
- Configure client groups
- Monitor forwarder management activities

Monitor Inputs

- Create file and directory monitor inputs
- Use optional settings for monitor inputs
- Deploy a remote monitor input

Network and Scripted Inputs

- Create network (TCP and UDP) inputs
- Describe optional settings for network inputs
- Create a basic scripted input

Agentless Inputs

- Identify Windows input types and uses
- Describe HTTP Event Collector

Fine Tuning Inputs

- Understand the default processing that occurs during input phase
- Configure input phase options, such as sourcetype fine-tuning and character set encoding

Parsing Phase and Data

- Understand the default processing that occurs during parsing
- Optimize and configure event line breaking
- Explain how timestamps and time zones are extracted or assigned to events
- Use Data Preview to validate event creation during the parsing phase

Manipulating Raw Data

- Explain how data transformations are defined and invoked
- Use transformations with props.conf and transforms.conf to:
    a. Mask or delete raw data as it is being indexed

b. Override sourcetype or host based upon event values
c. Route events to specific indexes based on event content
d. Prevent unwanted events from being indexed

- Use SEDCMD to modify raw data

Splunk Development

Use Forms

- Explain how tokens work
- Define types of token filters

Improve Performance

- Use the tstats command
- Use global searches

Customize Dashboards

- Customize panel link buttons
- Set panel refresh and delay times

Use Event Handlers

- Identify types of event handlers
- Describe event actions

Add Drilldowns

- Define types of drilldowns
- Identify predefined tokens

Add Advanced Visualizations & Behaviors

- Describe simple XML extensions
- Describe Splunk Custom Visualizations

Planning App Development

- Describe ways to monitor app performance

- Identify useful Splunk log files
- Describe security best practices

Creating Apps

- Define the app directory structure
- Describe app permissions

Adding Data

- List types of data inputs
- Describe add-ons

Creating a KV Store

- Define what is a KV Store
- Describe KV Store lookup
- Create a KV Store collection
- Search a KV Store collection
- Update content in a KV Store collection
- Delete a KV Store collection

Packaging Apps

- Describe the difference between local and default directories

Introduction to the Splunk REST API

- Describe the REST URI format
- Identify which Splunk server to connect to (e.g., search head, indexer, forwarder)
- Identify where REST logging occurs
- Describe authentication methods

Namespaces and Object Management

- Describe namespaces and why they matter
- Describe how the servicesNS is used with namespaces and REST endpoints
- Describe access control lists
- Update access control lists

Parsing REST Output

- Describe how the Splunk REST API uses Atom Syndication
- Describe the entry element
- Describe the content element
- Describe how to control the output format

Searching

- Describe the importance of specifying fields in a search
- Describe options for specifying a search time range
- Describe blocking, oneshot, normal, and export searches
- Describe search jobs
- Create and manage search jobs
- Describe ways to improve search performance

Writing Data to Splunk

- Identify some options that are available when creating an index
- Create and manage indexes
- Describe the Splunk HTTP Event Collector (HEC)
- Describe HEC tokens and how they are used
- Describe indexer acknowledgement
- Create and use HEC tokens to get data into Splunk

Splunk SIEM (Security Information and Event Management)

Introduction to Splunk Security

- Splunk security Fundamentals
- Traditional security threats
- Concept of Security Data model
- Describing correlation searches

Investigation and Monitoring

- Monitor the dashboard
- Investigating of notable events using incident review dashboards
- Workflow investigation and relative actions on identified flow

Investigation

- Enterprise Security Model
- Managing, Visualizing and Coordinating incident investigations using Deployment of
- ES investigation timelines
- Using journals and timelines for documenting breach analysis
- Efforts required to mitigate the issues
- Security Posture
- Incident Review

Risk Analysis and Network Analysis

- Risk analysis and identification
- Risk dashboard utilization
- How to manage the risk scores for objects and users
- Network Analysis

Web Intelligence

- HTTP category analysis
- HTTP user agent analysis
- Analyzing traffic size for spotting new threats

About the Splunk Enterprise Security Framework

- Spam Assassin Architecture
- Email Filter Architecture
- ES Solution Architecture
- Various Templates

Threat Intelligence

- Inspecting threat intelligence content with threat artefact dashboard
- Monitoring malicious websites with threat activity dashboard

User Intelligence

- Anomaly dashboards for user role and access logs

- Identity and asset concepts

Creating and tuning correlation searche

- Implementing the add-ons with Splunk

Using the Various Features of SIEM

Deploying Splunk Security Framework on AWS

Prerequisites:

- Splunk Fundamentals 1
- Splunk Fundamentals 2
- Before taking this course, students should have experience and knowledge of basic web development fundamentals (HTML, CSS, Javascript).
- Basic knowledge in SQL queries and command line interface.
- Knowledge of Data Analytics concepts is beneficial but not essential.
- Must have good knowledge of system administration.

Who Can attend:

- Splunk classes are designed for specific roles such as Splunk Administrator, Developer, User, Knowledge Manager, or Architect.
- The "Splunk Developer" course is targeted for Splunk users that want to create custom apps and visualizations in Splunk.
- Individual Contributors/Architects willing to implement Splunk in their organizations

Number of Hours: 50hrs

Certification:

- Splunk Enterprise Certified Admin
- Splunk Certified Developer

Key Features:

- One to One Training
- Online Training
- Fastrack & Normal Track

- Resume Modification
- Mock Interviews
- Video Tutorials
- Materials
- Real Time Projects
- Virtual Live Experience
- Preparing for Certification