Splunk Enterprise Certified Admin

Exam Description: The Splunk Enterprise Certified Admin exam is the final step towards completion of the Splunk Enterprise Certified Admin certification. This upper-level certification exam is a 57-minute, 60-question assessment which evaluates a candidate's knowledge and skills to manage various components of Splunk on a daily basis, including the health of the Splunk installation. Candidates can expect an additional 3 minutes to review the exam agreement, for a total seat time of 60 minutes. Candidates for this certification must complete the lecture, hands-on labs, and quizzes that are part of the Splunk Enterprise System Administration and Splunk Enterprise Data Administration courses in order to be eligible for the certification exam. Splunk Enterprise Certified Admin is a required prerequisite to the Splunk Enterprise Certified Architect and Splunk Certified Developer certification tracks.

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. The course provides content about Splunk forwarders and methods to get remote data into Splunk.

The following content areas are general guidelines for the content to be included on the exam:

- Splunk deployment overview
- License management
- Splunk apps
- Splunk configuration files
- Users, roles, and authentication
- Getting data in
- Distributed search
- Introduction to Splunk clusters
- Deploy forwarders with Forwarder Management
- Configure common Splunk data inputs
- Customize the input parsing process

The following topics are general guidelines for the content likely to be included on the exam; however, other related topics may also appear on any specific delivery of the exam. In order to better reflect the contents of the exam and for clarity purposes, the guidelines below may change at any time without notice.

1.0 Splunk Admin Basics **5%**

1.1 Identify Splunk components

2.0 License Management 5%

2.1 Identify license types
2.2 Understand license violations

3.0 Splunk Configuration Files 5%

3.1 Describe Splunk configuration directory structure
3.2 Understand configuration layering
3.3 Understand configuration precedence
3.4 Use btool to examine configuration settings

4.0 Splunk Indexes 10%

4.1 Describe index structure
4.2 List types of index buckets
4.3 Check index data integrity
4.4 Describe indexes.conf options
4.5 Describe the fishbucket
4.6 Apply a data retention policy

5.0 Splunk User Management 5%

5.1 Describe user roles in Splunk
5.2 Create a custom role
5.3 Add Splunk users

6.0 Splunk Authentication Management 5%

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

7.0 Getting Data In 5%

7.1 Describe the basic settings for an input
7.2 List Splunk forwarder types
7.3 Configure the forwarder
7.4 Add an input to UF using CLI

8.0 Distributed Search	**10%**

8.1 Describe how distributed search works
8.2 Explain the roles of the search head and search peers
8.3 Configure a distributed search group
8.4 List search head scaling options

9.0 Getting Data In – Staging	**5%**

9.1 List the three phases of the Splunk Indexing process
9.2 List Splunk input options

10.0 Configuring Forwarders	**5%**

10.1 Configure Forwarders
10.2 Identify additional Forwarder options

11.0 Forwarder Management	**10%**

11.1 Explain the use of Deployment Management
11.2 Describe Splunk Deployment Server
11.3 Manage forwarders using deployment apps
11.4 Configure deployment clients
11.5 Configure client groups
11.6 Monitor forwarder management activities

12.0 Monitor Inputs	**5%**

12.1 Create file and directory monitor inputs
12.2 Use optional settings for monitor inputs
12.3 Deploy a remote monitor input

13.0 Network and Scripted Inputs	**5%**

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

14.0 Agentless Inputs 5%

14.1 Identify Windows input types and uses
14.2 Describe HTTP Event Collector

15.0 Fine Tuning Inputs 5%

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

16.0 Parsing Phase and Data 5%

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

17.0 Manipulating Raw Data 5%

17.1 Explain how data transformations are defined and invoked
17.2 Use transformations with props.conf and transforms.conf to:

- Mask or delete raw data as it is being indexed
- Override sourcetype or host based upon event values
- Route events to specific indexes based on event content
- Prevent unwanted events from being indexed

17.3 Use SEDCMD to modify raw data