splunk>

Splunk Core Certified Power User

Exam Description: The Splunk Core Certified Power User exam is the final step towards completion of the Splunk Core Certified Power User certification. This next-level certification exam is a 57-minute, 65-question assessment which evaluates a candidate's knowledge and skills of field aliases and calculated fields, creating tags and event types, using macros, creating workflow actions and data models, and normalizing data with the CIM. Candidates can expect an additional 3 minutes to review the exam agreement, for a total seat time of 60 minutes. It is recommended that candidates for this certification complete the lecture, hands-on labs, and quizzes that are part of the Splunk Fundamentals 2 course in order to be prepared for the certification exam. Splunk Core Certified Power User is a required prerequisite to the Splunk Enterprise Certified Admin certification track.

This course focuses on searching and reporting commands, as well as on the creation of knowledge objects. Major topics include using transforming commands and visualizations, filtering and formatting results, correlating events, creating knowledge objects, using field aliases and calculated fields, creating tags and event types, using macros, creating workflow actions and data models, and normalizing data with the Common Information Model (CIM).

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

- Transforming commands and visualizations
- Filtering and formatting results
- Correlating events
- Knowledge objects
- Fields (field aliases, field extractions, calculated fields)
- Tags and event types
- Macros
- Workflow actions
- Data models
- Splunk Common Information Model (CIM)

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 Using Transforming Commands for Visualizations **5%**

1.1 Use the chart command
1.2 Use the timechart command

2.0 Filtering and Formatting Results **10%**

- 2.1 The eval command
- 2.2 Use the search and where commands to filter results
- 2.3 The fillnull command

3.0 Correlating Events **15%**

- 3.1 Identify transactions
- 3.2 Group events using fields
- 3.3 Group events using fields and time
- 3.4 Search with transactions
- 3.5 Report on transactions
- 3.6 Determine when to use transactions vs. stats

4.0 Creating and Managing Fields **10%**

- 4.1 Perform regex field extractions using the Field Extractor (FX)
- 4.2 Perform delimiter field extractions using the FX

5.0 Creating Field Aliases and Calculated Fields **10%**

- 5.1 Describe, create, and use field aliases
- 5.2 Describe, create, and use calculated fields

6.0 Creating Tags and Event Types **10%**

- 6.1 Create and use tags
- 6.2 Describe event types and their uses
- 6.3 Create an event type

7.0 Creating and Using Macros **10%**

- 7.1 Describe macros
- 7.2 Create and use a basic macro
- 7.3 Define arguments and variables for a macro
- 7.4 Add and use arguments with a macro

8.0 Creating and Using Workflow Actions **10%**

- 8.1 Describe the function of GET, POST, and Search workflow actions
- 8.2 Create a GET workflow action
- 8.3 Create a POST workflow action
- 8.4 Create a Search workflow action

9.0 Creating Data Models **10%**

- 9.1 Describe the relationship between data models and pivot
- 9.2 Identify data model attributes
- 9.3 Create a data model

10.0 Using the Common Information Model (CIM) Add-On **10%**

- 10.1 Describe the Splunk CIM
- 10.2 List the knowledge objects included with the Splunk CIM Add-On
- 10.3 Use the CIM Add-On to normalize data