Splunk Core Certified Advanced Power User

The Splunk Core Certified Advanced Power User exam is the final step toward completion of the Splunk Core Certified Advanced Power User certification.

70 Questions

Intermediate-Level

60* Minutes

Total exam time* ***includes 3 minutes* *to review the* ***exam agreement.***

Exam Content

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 Exploring Statistical Commands 4%

1.1 Performing statistical analysis with stats function
1.2 Using fieldsummary
1.3 Using appendpipe
1.4 Using count and list functions
1.5 Using eventstats
1.6 Using streamstats

2.0 Exploring eval Command Functions 4%

2.1 Using conversion functions
2.2 Using text functions
2.3 Using comparison and conditional functions
2.4 Using informational functions
2.5 Using statistical functions
2.6 Using makeresults command

3.0 Exploring Lookups 4%

3.1 Applying advanced lookup options
3.2 Including and excluding events based on lookup values
3.3 Using KV Store lookups
3.4 Using external lookups
3.5 Using geospatial lookups
3.6 Understanding best practices for lookups

4.0 Exploring Alerts 4%

4.1 Logging and indexing searchable alert events
4.2 Referencing lookups in alerts
4.3 Outputting alert results to a lookup
4.4 Using a webhook alert action
4.5 Creating a log event alert action

5.0 Advanced Field Creation and Management 4%

5.1 Identifying field extraction methods
5.2 Providing a regex expression to the Field Extractor to extract a field
5.3 Performing search time field extraction using the erex and rex commands
5.4 Understand how to improve regex performance in Splunk

6.0 Working with Self-Describing Data and Files 3%

6.1 Understanding self-describing data
6.2 Using the spath command
6.3 Using the eval command with the spath function
6.4 Using the multikv command

7.0 Advanced Search Macros 3%

7.1 Using nested search macros
7.2 Previewing search macros before executing
7.3 Using other knowledge objects with macros

8.0 Using Acceleration Options: Reports and Summary Indexing 4%

8.1 Describing acceleration
8.2 Identifying which reports qualify for acceleration
8.3 Identifying when Splunk doesn’t build an acceleration summary
8.4 Accelerating a report
8.5 Using the Report Acceleration Summaries and Summary Detail pages
8.6 Understanding summary Indexing
8.7 Using the summary indexing transforming commands
8.8 Defining searching against a summary
8.9 Understanding how to handle gaps and overlaps in summary indexes

9.0 Using Acceleration Options: Data Models and tsidx Files 4%

9.1 Exploring data models using the datamodel command
9.2 Understanding data model acceleration
9.3 Accelerating data models
9.4 Understanding tsidx files
9.5 Working with tsidx files using tstats commands
9.6 Using tstats to search accelerated data models
9.7 Determining which acceleration option to use

10.0 Using Search Efficiently 4%

10.1 Splunk architecture components
10.2 Search flow
10.3 Streaming commands
10.4 Transforming commands
10.5 Command ordering
10.6 Job inspector

11.0 More Search Tuning 3%

11.1 Pre-Filtering search data
11.2 Lispy and boolean operators
11.3 Lispy and wildcards
11.4 Using the TERM directive

12.0 Manipulating and FIltering Data 6%

12.1 bin command
12.2 xyseries command
12.3 untable command
12.4 foreach command
12.5 strftime function

13.0 Working with Multivalued Fields 7%

13.1 Multivalued fields
13.2 Some multivalued eval functions
13.3 makemv command
13.4 mvexpand command

14.0 Using Advanced Transactions 5%

14.1 Evaluating events to create transactions
14.2 Handling common values/different field names
14.3 An alternative to coalesce
14.4 Identifying complete vs. incomplete transactions
14.5 Making transactions more efficient
14.6 stats and transactions

15.0 Working with Time 2%

15.1 Using time effectively
15.2 What are the default time fields

16.0 Using Subsearches 6%

16.1 Filtering through many results
16.2 Subsearch caveats
16.3 When to use subsearch
16.4 When NOT to use subsearch
16.5 Troubleshooting subsearches
16.6 append command

17.0 Creating a Prototype 4%

17.1 Define simple XML syntax for views
17.2 Use best practices for creating views
17.3 Troubleshooting views

18.0 Using Forms 5%

18.1 Explain how tokens work
18.2 Use tokens with form inputs
18.3 Create cascading inputs
18.4 Define types of token filters

19.0 Improving Performance 6%

19.1 Identify ways to improve dashboard performance
19.2 Use the tstats command
19.3 Create base and post-process searches

20.0 Customizing Dashboards 6%

20.1 Customize chart and panel properties
20.2 Set panel refresh and delay times
20.3 Disable search access features
20.4 Create event annotations

21.0 Adding Drilldowns 7%

21.1 Define types of drilldowns
21.2 Identify predefined tokens
21.3 Create dynamic drilldowns

22.0 Adding Advanced Behaviors and Visualizations 5%

22.1 Identify types of event handlers
22.2 Define event actions
22.3 Create contextual drilldowns

22.4 Use simple XML extensions

Exam Preparation

Candidates may reference the Splunk How-To YouTube Channel, Splunk Docs, and draw from their own Splunk experience.

The following is a ***suggested and non-exhaustive*** list of training from the Core Certified Advanced Power User Learning Path that may cover topics listed in the above blueprint:

❏ Using Fields

❏ Working with Time

❏ Comparing Values

❏ Result Modification

❏ Leveraging Lookups and Subsearches

❏ Correlation Analysis

❏ Multivalue Fields

❏ Search Optimization

❏ Creating Knowledge Objects

❏ Creating Field Extractions

❏ Enriching Data with Lookups

❏ Data Models

❏ Introduction to Dashboards

❏ Dynamic Dashboards

The prerequisite exam for this certification is:

□ Splunk Core Certified Power User

Schedule this exam >