splunk>

Splunk Certified Developer

Exam Description: The Splunk Certified Developer exam is the final step towards completion of the Splunk Certified Developer certification. This highly technical certification exam is a 57-minute, 50-question assessment which evaluates a candidate's knowledge and skills in drilldowns, advanced behaviors and visualizations, building apps using the Splunk Web Framework, and REST endpoints. Candidates can expect an additional 3 minutes to review the exam agreement, for a total seat time of 60 minutes. The prerequisite exams for this certification are Splunk Core Certified Power User and **either** Splunk Enterprise Certified Admin **or** Splunk Cloud Certified Admin. It is recommended that candidates for this certification complete the lecture, hands-on labs, and quizzes that are part of the Creating Dashboards with Splunk*, Advanced Dashboards & Visualizations, Building Splunk Apps, and Developing with Splunk's REST API courses in order to be prepared for the certification exam.

**Candidates may also choose to complete the following courses in lieu of Creating Dashboards:*

- ❏ *Introduction to Dashboards*
- ❏ *Dynamic Dashboards*
- ❏ *Using Choropleth*

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 Use Forms **5%**

- 1.1 Explain how tokens work
- 1.2 Define types of token filters

2.0 Improve Performance **5%**

- 2.1 Use the tstats command
- 2.2 Use global searches

3.0 Customize Dashboards **5%**

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

4.0 Use Event Handlers **5%**

- 4.1 Identify types of event handlers
- 4.2 Describe event actions

5.0 Add Drilldowns **5%**

- 5.1 Define types of drilldowns
- 5.2 Identify predefined tokens

6.0 Add Advanced Visualizations & Behaviors **5%**

- 6.1 Describe simple XML extensions
- 6.2 Describe Splunk Custom Visualizations

7.0 Planning App Development **10%**

- 7.1 Describe ways to monitor app performance
- 7.2 Identify useful Splunk log files
- 7.3 Describe security best practices

8.0 Creating Apps **5%**

- 8.1 Define the app directory structure
- 8.2 Describe app permissions

9.0 Adding Data **5%**

- 9.1 List types of data inputs
- 9.2 Describe add-ons

10.0 Creating a KV Store **5%**

- 10.1 Define what is a KV Store
- 10.2 Describe KV Store lookup
- 10.3 Create a KV Store collection
- 10.4 Search a KV Store collection
- 10.5 Update content in a KV Store collection
- 10.6 Delete a KV Store collection

11.0 Packaging Apps **5%**

- 11.1 Describe the difference between local and default directories

12.0 Introduction to the Splunk REST API **5%**

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

13.0 Namespaces and Object Management **10%**

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

14.0 Parsing REST Output **5%**

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

15.0 Searching **10%**

- 15.1 Describe the importance of specifying fields in a search
- 15.2 Describe options for specifying a search time range
- 15.3 Describe oneshot, normal, and export searches
- 15.4 Describe search jobs
- 15.5 Create and manage search jobs
- 15.6 Describe ways to improve search performance

16.0 Writing Data to Splunk **10%**

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