Splunk Cloud Certified Admin

The Splunk Cloud Certified Admin exam is the final step towards completion of the Splunk Cloud Certified Admin certification track.

60 Questions	Professional-Level	75* 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 Splunk Cloud Overview 5%

- 1.1 Describe Cloud topology
- 1.2 Describe tasks managed by the Splunk cloud administrator
- 1.3 List the primary differences between Splunk Cloud and Splunk Enterprise
- 1.4 List differences between Self-Service Cloud and Managed Cloud

2.0 Index Management 5%

- 2.1 Define a Splunk index
- 2.2 Create indexes in cloud
- 2.3 Delete data from an index
- 2.4 Monitor indexing activities

3.0 User Authentication and Authorization 5%

- 3.1 Administer Splunk user roles

3.2 Integrate Splunk with LDAP, Active Directory, or SAML

4.0 Splunk Configuration Files 5%

4.1 Review Splunk configuration files and directories
4.2 Review configuration file precedence
4.3 Review index and search time processes

5.0 Getting Data in Cloud 15%

5.1 List Splunk forwarder types
5.2 Describe the role of forwarders
5.3 Configure a forwarder to Splunk Cloud
5.4 Test the forwarder connection
5.5 Describe optional forwarder settings

6.0 Forwarder Management 5%

6.1 Describe Splunk Deployment Server
6.2 Explain the use of forwarder management
6.3 Configure forwarders to be deployment clients
6.4 Managing forwarders using deployment apps

7.0 Monitor Inputs 15%

7.1 Describe the Splunk process for inputting data
7.2 Create file and directory monitor inputs
7.3 Use optional settings for monitor inputs

8.0 Network and Other Inputs 10%

8.1 Create network (TCP and UDP) inputs
8.2 Create a basic scripted input
8.3 Describe optional settings for network inputs
8.4 Identify Windows input types and uses

8.5 Use the HTTP Event Collector (HEC) to get data into Splunk

9.0 Fine-tuning Inputs 5%

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

10.0 Parsing Phase and Data Preview 10%

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

11.0 Manipulating Raw Data 10%

11.1 Explain how data transformations are defined and invoked
11.2 Use transformations with props.conf and transforms.conf to modify raw data
11.3 Use SEDCMD to modify raw data

12.0 Installing and Managing Apps 5%

12.1 Review the process for installing apps
12.2 Describe private apps
12.3 Describe how apps are managed

13.0 Working with Splunk Cloud Support 5%

13.1 Isolate problems before contacting Splunk Cloud Support
13.2 Define the process for working with Splunk Cloud Support

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 Cloud Certified Admin Learning Path that may cover topics listed in the above blueprint:

- ❏ Splunk Cloud Administration
  for net-new Splunk Administrators
- ❏ Transitioning to Splunk Cloud
  for experienced Enterprise Administrators moving to Splunk Cloud

The prerequisite exam for this certification is:

- ☐ Splunk Core Certified Power User

Schedule this exam >