splunk>

Splunk Core Certified Consultant

Exam Description: The Splunk Core Certified Consultant certification exam is the final step in the Splunk Core Certified Consultant track. This highly technical certification exam is a 117-minute, 86-question assessment which evaluates a candidate's knowledge and skills in Splunk Deployment Methodology and best-practices for planning, data collection, and sizing, managing, and troubleshooting a standard with indexer and search head clustering. Candidates can expect an additional 3 minutes to review the exam agreement, for a total seat time of 120 minutes. Candidates interested in this certification must complete the lecture, hands-on labs, and quizzes that are part of the Fundamentals 3, Creating Dashboards with Splunk, and Advanced Searching and Reporting courses by Splunk Education, the Indexer Cluster Implementation Lab, the Distributed Search Migration Lab, the Implementation Fundamentals Lab, the Architect Implementation Labs (1-3), as well as the Services: Core Implementation Instructor-Led Training course in order to be eligible for the certification exam. The prerequisite exams for this certification are Splunk Core Certified Power User, Splunk Enterprise Certified Admin, and Splunk Enterprise Certified Architect.

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

- Splunk Validated Architectures
- Monitoring Console configuration
- Authentication Protocols
- Splunk to Splunk (S2S) Communication
- Data Inputs
- Forwarder Types
- HEC Tokens
- Fishbucket Records
- Pretrained Sourcetypes
- Indexing Buckets
- Event Processing
- Indexing Intervals
- Data Retention
- Search Head Dispatch
- Sub-searches
- Deployment Apps
- Deployment Server
- Indexer Clustering
- Upgrading an Indexer Cluster
- Indexer Cluster Failure Modes
- Multi-site Clustering
- Indexer Migration
- Search Head Clustering

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 Deploying Splunk **5%**

- 1.1 Define Splunk Validated Architectures
- 1.2 Articulate how and why Splunk grows from standalone environment to distributed environment with indexer and Search Head clustering
- 1.3 Explain the difference between High Availability and Disaster Recovery and how both can be addressed in Splunk.

2.0 Monitoring Console **8%**

- 2.1 Describe which instances are suitable to configure as the Monitoring Console
- 2.2 Articulate how to configure the MC for a single or distributed environment
- 2.3 Examine how the MC uses the server roles and groups
- 2.4 Describe how MC health checks are performed and can be extended.

3.0 Access and Roles **8%**

- 3.1 Identify authentication methods
- 3.2 Describe LDAP concepts and configuration
- 3.3 List SAML and SSO options
- 3.4 Define roles and articulate how roles are used to secure data

4.0 Data Collection **15%**

- 4.1 Articulate the different ways data can be ingested by an indexer
- 4.2 Articulate how one Splunk instance communicates with another Splunk instance (S2S)
- 4.3 Describe the types and configuration of data inputs
- 4.4 Describe ways to troubleshoot data inputs

5.0 Indexing **14%**

- 5.1 List indexing artefacts and locations
- 5.2 Describe event processing and data pipelines
- 5.3 Describe the underlying text parsing and indexing process
- 5.4 List data retention controls

6.0 Search **14%**

- 6.1 Describe how to use search job inspection, Explain the inner-workings of a search
- 6.2 List the different search types
- 6.3 Describe how to maximize search efficiency
- 6.4 Describe how sub-searches work

7.0 Configuration Management **8%**

- 7.1 Describe a deployment app
- 7.2 Articulate how a Deployment Server works
- 7.3 Describe deployment system configuration
- 7.4 Articulate how to manage deployment Server

8.0 Indexer Clustering **18%**

- 8.1 Describe deployment and component configuration
- 8.2 Describe the life cycle of data using buckets
- 8.3 Determine failure modes and recovery processes
- 8.4 Articulate how multi-site clustering works
- 8.5 List migration procedures

9.0 Search Head Clustering **10%**

- 9.1 Articulate how to manage and deploy a Search Head cluster
- 9.2 Determine when a Search Head Cluster may be needed and when a Search Head Cluster would not be recommended
- 9.3 Describe content management using the Deployer
- 9.4 Describe the role of the cluster members and the Captain
- 9.5 Articulate how Captain election works (RAFT)