Splunk Enterprise Certified Architect

Exam Description: The Splunk Enterprise Certified Architect exam is the final step towards completion of the Splunk Enterprise Certified Architect certification. This highly technical certification exam is an 87-minute, 85-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 90 minutes. Candidates for this certification must complete the lecture, hands-on labs, and quizzes that are part of the Architecting Splunk Enterprise Deployments, Troubleshooting Splunk Enterprise, and Splunk Enterprise Cluster Administration courses, as well as the Splunk Enterprise Deployment Practical Lab in order to be eligible for the certification exam. The prerequisite exams for this certification are Splunk Core Certified Power User and Splunk Enterprise Certified Admin.

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

- Requirements definition
- Index and infrastructure planning
- Clustering Overview
- Forwarder and Deployment
- Integration
- Splunk Support model
- Splunk troubleshooting methods and tools
- Clarifying the problem, installation, licensing, and crash problems
- UI and search problems
- Configuration problems
- Deployment problems
- User management problems
- Large-scale Splunk deployment overview
- Single-site (high-availability) indexer cluster, multi-site (disaster-recovery) indexer cluster
- Indexer cluster management and administration
- Indexer discovery forwarder configuration
- Search head cluster
- Search head cluster management and administration
- KV Store collection and lookup management

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 Introduction **2%**

- 1.1 Describe a deployment plan
- 1.2 Define the deployment process

2.0 Project Requirements **5%**

- 2.1 Identify critical information about environment, volume, users, and requirements
- 2.2 Apply checklists and resources to aid in collecting requirements

3.0 Infrastructure Planning: Index Design **5%**

- 3.1 Understand design and size indexes
- 3.2 Estimate non-smart store related storage requirements
- 3.3 Identify relevant apps

4.0 Infrastructure Planning: Resource Planning **7%**

- 4.1 List sizing considerations
- 4.2 Identify disk storage requirements
- 4.3 Define hardware requirements for various Splunk components
- 4.4 Describe ES considerations for sizing and topology
- 4.5 Describe ITSI considerations for sizing and topology
- 4.6 Describe security, privacy, and integrity measures

5.0 Clustering Overview **5%**

- 5.1 Identify non-smart store related storage and disk usage requirements
- 5.2 Identify search head clustering requirements

6.0 Forwarder and Deployment Best Practices **6%**

- 6.1 Identify best practices for forwarder tier design
- 6.2 Understand configuration management for all Splunk components, using Splunk deployment tools

7.0 Performance Monitoring and Tuning **5%**

- 7.1 Use limits.conf to improve performance
- 7.2 Use indexes.conf to manage bucket size
- 7.3 Tune props.conf
- 7.4 Improve search performance

8.0 Splunk Troubleshooting Methods and Tools **5%**

- 8.1 Splunk diagnostic resources and tools

9.0 Clarifying the Problem **5%**

- 9.1 Identify Splunk's internal log files
- 9.2 Identify Splunk's internal indexes

10.0 Licensing and Crash Problems **5%**

- 10.1 License issues
- 10.2 Crash issues

11.0 Configuration Problems **5%**

- 11.1 Input issues

12.0 Search Problems **5%**

- 12.1 Search issues
- 12.2 Job inspector

13.0 Deployment Problems **5%**

- 13.1 Forwarding issues
- 13.2 Deployment server issues

14.0 Large-scale Splunk Deployment Overview **5%**

- 14.1 Identify Splunk server roles in clusters
- 14.2 License Master configuration in a clustered environment

15.0 Single-site Indexer Cluster **5%**

15.1 Splunk single-site indexer cluster configuration

16.0 Multisite Indexer Cluster **5%**

16.1 Splunk multisite indexer cluster overview
16.2 Multisite indexer cluster configuration
16.3 Cluster migration and upgrade considerations

17.0 Indexer Cluster Management and Administration **7%**

17.1 Indexer cluster storage utilization options
17.2 Peer offline and decommission
17.3 Master app bundles
17.4 Monitoring Console for indexer cluster environment

18.0 Search Head Cluster **5%**

18.1 Splunk search head cluster overview
18.2 Search head cluster configuration

19.0 Search Head Cluster Management and Administration **5%**

19.1 Search head cluster deployer
19.2 Captaincy transfer
19.3 Search head member addition and decommissioning

20.0 KV Store Collection and Lookup Management **3%**

20.1 KV Store collection in Splunk clusters