splunk>
certification

Splunk Certification

Certification Exam Study Guide

Splunk Certification Exams

Table of Contents

Please note: These sample questions are provided to give candidates a general idea of the formatting and type of questions for each of the exams listed above. The test blueprints (linked for each specific exam in the following pages) provide much more detailed information regarding exam content. **Candidate performance on these questions in no way guarantees performance or passing marks on the certification exam(s).**

Splunk Certification Exams

Sample Questions - Splunk Core Certified User

For a detailed breakdown of the exam content, please see the **Splunk Core Certified User Test Blueprint**.

1. Which of the following is a main processing component of basic Splunk architecture?
   a. Indexer
   b. Load balancer
   c. License master
   d. Deployment server

2. According to Splunk best practices, which of the following searches is most efficient if we are interested in searching the Windows Security Event Log for failures?
   a. `status=failure`
   b. `index=oswinsec sourcetype=WinEventLog:Security status=failure`
   c. `index=oswinsec sourcetype=WinEventLog:* status=failure`
   d. `index=oswinsec failure`

3. Which search command calculates statistics based on fields in the events?
   a. `top`
   b. `rare`
   c. `stats`
   d. `fields`

Splunk Certification Exams

Answer Key - Splunk Core Certified User

For a detailed breakdown of the exam content, please see the **Splunk Core Certified User Test Blueprint**.

1.	A
2.	B
3.	C

Splunk Certification Exams

Sample Questions - Splunk Core Certified Power User

For a detailed breakdown of the exam content, please see the [Splunk Core Certified Power User Test Blueprint]().

1. Which command is used **only** to create a time series visualization?
   a. `_time`
   b. `chart`
   c. `timechart`
   d. `timeseries`

2. Which of the following statements describe field aliases? (select all that apply)
   a. Field aliases are applied after lookups.
   b. Field aliases can be applied to lookups.
   c. Multiple aliases can be applied to one field.
   d. The original field is not replaced by the field alias.

3. What action type is used when creating a POST workflow action?
   a. Web
   b. Link
   c. HTTP
   d. HTTPS

Splunk Certification Exams

Answer Key - Splunk Core Certified Power User

For a detailed breakdown of the exam content, please see the **Splunk Core Certified Power User Test Blueprint**.

1. C
2. B, C, D
3. B

Splunk Certification Exams

Sample Questions - Splunk Enterprise Certified Admin

For a detailed breakdown of the exam content, please see the Splunk Enterprise Certified Admin Test Blueprint.

1. Which Splunk component receives, indexes, and stores incoming data from forwarders?
   a. Indexer
   b. Search head
   c. Cluster master
   d. Deployment server

2. Which license type allows 500MB/day of indexing, but disables alerts, authentication, cluster, distributed search, summarization, and forwarding to non-Splunk servers?
   a. Free license
   b. Forwarder license
   c. Enterprise license
   d. Enterprise trial license

3. What can be used when setting the host field option on a network input? (select all that apply)
   a. IP
   b. DNS
   c. A binary file
   d. Custom (explicit value)

Splunk Certification Exams

Answer Key - Splunk Enterprise Certified Admin

For a detailed breakdown of the exam content, please see the **Splunk Enterprise Certified Admin Test Blueprint**.

1. A
2. A
3. A, B, D

Splunk Certification Exams

Sample Questions - Splunk Enterprise Certified Architect

For a detailed breakdown of the exam content, please see the [Splunk Enterprise Certified Architect Test Blueprint]().

1. Search mode is a setting that optimizes search performance by controlling the amount or type of data that the search returns. Which of the following are valid search mode settings? (select all that apply)
   a. Fast
   b. Smart
   c. Verbose
   d. Transform

2. By default, what is the retention period for the Splunk `_audit` index?
   a. 14 days
   b. 30 days
   c. 90 days
   d. 6 years

3. All Splunk users are unable to run searches. A legacy license file is suspected to have caused the issue. Which Splunk log component could be used to clarify and confirm the issue?
   a. `Metrics`
   b. `LMStackMgr`
   c. `ServerConfig`
   d. `SearchProcessRunner`

Splunk Certification Exams

Answer Key - Splunk Enterprise Certified Architect

For a detailed breakdown of the exam content, please see the Splunk Enterprise Certified Architect Test Blueprint.

1. A, B, C
2. D
3. B