Splunk Certification

Certification Exam Study Guide

splunk> turn data into doing™

Splunk Certification Exams

Quick Reference Guide

For registration assistance, please see our Exam Registration Tutorial.

Exam registration costs **$125**. This fee applies to **each exam attempt**.

Exams are available in-person at Pearson VUE testing centers (hint: click the “Find a Test Center” link in the right-hand sidebar) or via **Online Proctor** (strict requirements apply - see here for more details).

To change or cancel an existing appointment less than 48 hours in advance, please contact Pearson VUE Customer Support directly. All other appointment changes can be made via your Pearson VUE account.

When sitting for a certification exam, candidates will have **3 minutes to review and accept the Splunk Certification Agreement**. Exam sessions will be terminated if this is not accepted within the designated time-frame. Candidates can review the agreement in detail at their convenience via our Splunk Certification Candidate Handbook (page 14).

For an overview of **exam duration and number of questions**, please see here.

Splunk Certification Exams

Table of Contents

Please note: Sample questions (where available) 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 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).

Core, Cloud, Enterprise Offerings

splunk> turn data into doing

Splunk Certification Exams

Table of Contents

Please note: Sample questions (where available) 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 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).

App-Specific Offerings

Splunk Enterprise Security Certified Admin

- Sample Questions
- Test Blueprint

Splunk IT Service Intelligence Certified Admin

- Sample Questions
- Test Blueprint

Splunk Phantom Certified Admin

- Test Blueprint

Splunk Certified Developer

- Sample Questions
- Test Blueprint

Splunk Core Certified User

Sample Questions

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 Core Certified User

Answer Key

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 Core Certified Power User

Sample Questions

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 are applied before lookups.
   c. Field aliases can be applied to lookups.
   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 Core Certified Power User

Answer Key

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 are applied before lookups.
   - [✓ c.] Field aliases can be applied to lookups.
   - [✓ 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 Enterprise Certified Admin

Sample Questions

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 Enterprise Certified Admin

Answer Key

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 Enterprise Certified Architect

Sample Questions

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 Enterprise Certified Architect

Answer Key

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 Enterprise Security Certified Admin

Sample Questions

1. When is it appropriate to use Auto Deployment on `Splunk_TA_ForIndexers`in a distributed search configuration?
   a. When the indexers are clustered.
   b. When there are multiple indexers with the same retention settings.
   c. When there are multiple indexers with the same storage volume settings.
   d. When there are multiple indexers with different volume and retention settings.

2. In order for ES to automatically take an action upon locating a particular event, what can a correlation search be configured to execute?
   a. Action script
   b. Activation prompt
   c. Adaptive response
   d. Integration script

3. When creating a correlation search, which command will generate a notable event if the risk score for any one host is greater than 100?
   a. `| where 'risk_score' > 100`
   b. `| eval risk_score > 100`
   c. `| sum(host)risk_score > 100`
   d. `| All_Risk.risk_score > 100`

Splunk Enterprise Security Certified Admin

Answer Key

1. When is it appropriate to use Auto Deployment on `Splunk_TA_ForIndexers`in a distributed search configuration?
    a. When the indexers are clustered.
    b. When there are multiple indexers with the same retention settings.
    [✓ c.] When there are multiple indexers with the same storage volume settings.
    d. When there are multiple indexers with different volume and retention settings.

2. In order for ES to automatically take an action upon locating a particular event, what can a correlation search be configured to execute?
    a. Action script
    b. Activation prompt
    [✓ c.] Adaptive response
    d. Integration script

3. When creating a correlation search, which command will generate a notable event if the risk score for any one host is greater than 100?
    [✓ a.] `| where 'risk_score' > 100`
    b. `| eval risk_score > 100`
    c. `| sum(host)risk_score > 100`
    d. `| All_Risk.risk_score > 100`

Splunk IT Service Intelligence Certified Admin

Sample Questions

1. Which of the following accurately describes an individual notable event?
   a. It is immutable.
   b. It can be cloned.
   c. It can have its status changed.
   d. It can be assigned to an analyst.

2. Which of the following is an adaptive threshold best practice?
   a. Use if there is no consistent flow of data.
   b. Disable backfill on adaptive threshold data.
   c. Use when KPI values are expected to move dynamically.
   d. Update adaptive threshold values manually each day at midnight.

3. Within a correlation search, how can a service be associated?
   a. By using lookup in the ad hoc search.
   b. By modifying `correlation_searches.conf`
   c. By specifying an appropriate time range.
   d. By adding the service name to the service field.

Splunk IT Service Intelligence Certified Admin

Answer Key

1. Which of the following accurately describes an individual notable event?
   [✓ a.] It is immutable.
   b. It can be cloned.
   c. It can have its status changed.
   d. It can be assigned to an analyst.

2. Which of the following is an adaptive threshold best practice?
   a. Use if there is no consistent flow of data.
   b. Disable backfill on adaptive threshold data.
   [✓ c.] Use when KPI values are expected to move dynamically.
   d. Update adaptive threshold values manually each day at midnight.

3. Within a correlation search, how can a service be associated?
   a. By using lookup in the ad hoc search.
   b. By modifying `correlation_searches.conf`
   c. By specifying an appropriate time range.
   [✓ d.] By adding the service name to the service field.

Splunk Certified Developer

Sample Questions

1. What is a global search?
   a. A scheduled search or report shared for use in multiple dashboards.
   b. A search with tokens that have defaults set to all indexes or sources.
   c. An inline search or report on a dashboard to provide input for post-process searches.
   d. A single base search with post-process searches that populate all panels on a dashboard.

2. Simple XML extensions can be used for which of the following file types?
   a. JS, CSS
   b. CSS, EXE
   c. JS, CSS, DOC
   d. CSS, HTML, JS

3. To stop a search job with a `sid` of 1519670895.34, which REST request should be used?
   a. `/services/search/jobs/1519670895.34/command -d action=stop`
   b. `/services/search/jobs/1519670895.34/command -d action=remove`
   c. `/services/search/jobs/1519670895.34/control -d action=cancel`
   d. `/services/search/jobs/1519670895.34/control -d action=delete`

Splunk Certified Developer

Answer Key

1. What is a global search?
   - a. A scheduled search or report shared for use in multiple dashboards.
   - b. A search with tokens that have defaults set to all indexes or sources.
   - c. An inline search or report on a dashboard to provide input for post-process searches.
   - [✓ d.] A single base search with post-process searches that populate all panels on a dashboard.

2. Simple XML extensions can be used for which of the following file types?
   - [✓ a.] JS, CSS
   - b. CSS, EXE
   - c. JS, CSS, DOC
   - d. CSS, HTML, JS

3. To stop a search job with a `sid` of 1519670895.34, which REST request should be used?
   - a. `/services/search/jobs/1519670895.34/command -d action=stop`
   - b. `/services/search/jobs/1519670895.34/command -d action=remove`
   - [✓ c.] `/services/search/jobs/1519670895.34/control -d action=cancel`
   - d. `/services/search/jobs/1519670895.34/control -d action=delete`