Splunk Certification

Certification Exam Study Guide

splunk> turn data into doing™

Splunk Certification

Quick Link References

COVID-19 Exam Delivery Updates can be found [here](#).

Splunk Certification Candidate Handbook

Everything you need to know about the Splunk Certification program.

Splunk Certification Exam Agreement

All candidates must review and agree to this policy in-full prior to accessing a Splunk Certification Exam.

Exam Registration Tutorial

Step-by-step exam registration assistance with detailed screenshots of the registration process.

Online Proctored Delivery Overview

What to expect when taking a Splunk Certification exam via online proctor.

Contact Pearson VUE Support

Pearson VUE registration troubleshooting, account issues, or exam delivery issues.

splunk> turn data into doing
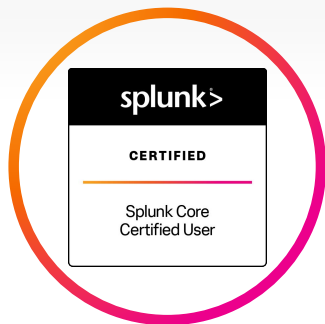
Splunk Certification Exams

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).

splunk> turn data into doing

Splunk Core Certified User

What's on the Exam

This entry-level certification exam is a 57-minute, 60-question assessment which evaluates a candidate's knowledge and skills to search, use fields, create alerts, use lookups, and create basic statistical reports and dashboards. Candidates can expect an additional 3 minutes to review the exam agreement, for a total seat time of 60 minutes.

Splunk Core Certified User is a recommended entry-level certification track for all candidates.

We recommend exam candidates complete Splunk Fundamentals 1 course or the following courses:

- ❏ What is Splunk?
- ❏ Intro to Splunk
- ❏ Using Fields
- ❏ Scheduling Reports and Alerts
- ❏ Visualizations
- ❏ Statistical Processing
- ❏ Working with Time
- ❏ Leveraging Lookups and Subsearches
- ❏ Search Optimization
- ❏ Enriching Data with Lookups
- ❏ Data Models

Looking for more details? Review the test blueprint here.

Prerequisite Certification(s):

- None

Prerequisite Course(s):

- None

Recommended Next Steps:

- Splunk Core Certified Power User

splunk> turn data into doing

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> turn data into doing

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> turn data into doing

Splunk Core Certified Power User

What's on the Exam

This next-level certification exam is a 57-minute, 65-question assessment which evaluates a candidate's knowledge and skills of field aliases and calculated fields, creating tags and event types, using macros, creating workflow actions and data models, and normalizing data with the CIM. Candidates can expect an additional 3 minutes to review the exam agreement, for a total seat time of 60 minutes.

In order to be prepared for the certification exam, Splunk recommends one of the following paths: the Splunk Fundamentals 2 course or the following courses:

- ❏ Visualizations
- ❏ Statistical Processing
- ❏ Working with Time
- ❏ Comparing Values
- ❏ Result Modification
- ❏ Correlation Analysis
- ❏ Search Under the Hood
- ❏ Introduction to Knowledge Objects
- ❏ Creating Knowledge Objects
- ❏ Creating Field Extractions
- ❏ Data Models
- ❏ Using Choropleth

Looking for more details? Review the test blueprint here.

Prerequisite Certification(s):

- None

Prerequisite Course(s):

- None

Recommended Next Steps:

- Splunk Core Certified Advanced Power User
- Splunk Enterprise Certified Admin
- Splunk Cloud Certified Admin

splunk> CERTIFIED

Splunk Core Certified Power User

splunk> turn data into doing

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> turn data into doing

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> turn data into doing

Splunk Core Certified Advanced Power User

What's on the Exam

This advanced certification exam is a 57-minute, 68-question assessment which evaluates a candidate's knowledge and skills in more advanced searching and reporting commands, advanced use cases of knowledge objects, and best practices for building dashboards and forms. Candidates can expect an additional 3 minutes to review the exam agreement, for a total seat time of 60 minutes.

In order to be prepared for the certification exam, Splunk recommends one of the following paths: completion of the Fundamentals 3, Creating Dashboards with Splunk, and Advanced Searching and Reporting or the following modules:

- ❏ Using Fields
- ❏ Working with Time
- ❏ Comparing Values
- ❏ Result Modification
- ❏ Leveraging Lookups and Subsearches
- ❏ Correlation Analysis
- ❏ Search Under the Hood
- ❏ Multivalue Fields
- ❏ Search Optimization
- ❏ Creating Field Extractions
- ❏ Enriching Data with Lookups
- ❏ Data Models
- ❏ Using Choropleth
- ❏ Introduction to Dashboards
- ❏ Dynamic Dashboards

Looking for more details? Review the test blueprint here.

Prerequisite Certification(s):

- Splunk Core Certified Power User

Prerequisite Course(s):

- None

Recommended Next Steps:

- Splunk Certified Developer
- Splunk Enterprise Certified Admin
- Splunk Cloud Certified Admin

splunk> turn data into doing

CERTIFIED

Splunk Cloud
Certified Admin

Prerequisite Certification(s):

● Splunk Core Certified Power User

Prerequisite Course(s):

● None

Recommended Next Steps:

● Splunk Certified Developer
● Splunk ES Certified Admin
● Splunk ITSI Certified Admin
● Splunk Phantom Certified Admin

Splunk Cloud Certified Admin

What's on the Exam

This upper-level certification exam is a 72-minute, 63-question assessment which evaluates a candidate's knowledge and skills in best practices and configuration details for Splunk Cloud, including data inputs and forwarder configuration, data management, user accounts, and basic monitoring and problem isolation. Candidates can expect an additional 3 minutes to review the exam agreement, for a total seat time of 75 minutes. It is recommended that candidates for this certification complete the lecture, hands-on labs, and quizzes that are part of the Splunk Cloud Administration or Transitioning to Splunk Cloud course in order to be prepared for the certification exam.

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

● Splunk Cloud overview
● Splunk index management
● Users, roles, and authentication
● Splunk configuration files
● Universal forwarder
● Forwarder management
● Data inputs in detail
● Event parsing with data preview
● Manipulating raw data
● Installing apps
● Problem isolation and Splunk Cloud support

Looking for more details? Review the test blueprint here.

splunk> turn data into doing

Splunk Enterprise Certified Admin

What's on the Exam

This upper-level certification exam is a 57-minute, 56-question assessment which evaluates a candidate's knowledge and skills to manage various components of Splunk on a daily basis, including the health of the Splunk installation. Candidates can expect an additional 3 minutes to review the exam agreement, for a total seat time of 60 minutes. It is recommended that candidates for this certification complete the lecture, hands-on labs, and quizzes that are part of the Splunk Enterprise System Administration and Splunk Enterprise Data Administration courses in order to be prepared for the certification exam.

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

- Splunk deployment overview
- License management
- Splunk apps
- Splunk configuration files
- Users, roles, and authentication
- Getting data in
- Distributed search
- Introduction to Splunk clusters
- Deploy forwarders with Forwarder Management
- Configure common Splunk data inputs
- Customize the input parsing process

Looking for more details? Review the test blueprint here.

Prerequisite Certification(s):

- Splunk Core Certified Power User

Prerequisite Course(s):

- None

Recommended Next Steps:

- Splunk Certified Developer
- Splunk Enterprise Certified Architect
- Splunk ES Certified Admin
- Splunk ITSI Certified Admin
- Splunk Phantom Certified Admin

splunk> turn data into doing

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> turn data into doing

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 > turn data into doing

Splunk Enterprise Certified Architect

What's on the Exam

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 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

Looking for more details? Review the test blueprint here.

Prerequisite Certification(s):

- Splunk Core Certified Power User
- Splunk Enterprise Certified Admin

Prerequisite Course(s):

- Architecting Splunk Enterprise Deployments
- Troubleshooting Splunk Enterprise
- Splunk Cluster Administration
- Splunk Deployment Practical Lab

Recommended Next Steps:

- Splunk Core Certified Consultant

splunk> turn data into doing

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> turn data into doing

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> turn data into doing

Splunk Core Certified Consultant

What's on the Exam

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. To qualify for the certification exam, candidates **must** complete 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 course. For a full list of exam eligibility requirements, please refer to the Splunk Core Certified Consultant track flowchart.

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

Looking for more details? Review the test blueprint here.

Prerequisite Certification(s):

- Splunk Core Certified Power User
- Splunk Enterprise Certified Admin
- Splunk Enterprise Certified Architect

Prerequisite Course(s):

- *Fundamentals 3, Creating Dashboards, Advanced Searching & Reporting**
- Core Consultant Labs
- Services: Core Implementation

Recommended Next Steps:

- None

*Candidates may substitute Splunk Core Certified Advanced Power User digital badge in lieu of courses.

splunk> turn data into doing

Splunk Certified Developer

What's on the Exam

This upper-level certification exam is a 57-minute, 56-question assessment which evaluates a candidate's knowledge and skills to manage various components of Splunk on a daily basis, including the health of the Splunk installation. Candidates can expect an additional 3 minutes to review the exam agreement, for a total seat time of 60 minutes. It is recommended that candidates for this certification complete the lecture, hands-on labs, and quizzes that are part of the Splunk Enterprise System Administration and Splunk Enterprise Data Administration courses in order to be prepared for the certification exam. It is recommended that candidates for this certification complete the lecture, hands-on labs, and quizzes that are part of the Creating Dashboards with Splunk*, Advanced Dashboards & Visualizations, Building Splunk Apps, and Developing with Splunk's REST API courses in order to be prepared for the certification exam.

Candidates may also choose to complete the following courses in lieu of Creating Dashboards:
- ❏ *Introduction to Dashboards*
- ❏ *Dynamic Dashboards*
- ❏ *Using Choropleth*

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

- Splunk deployment overview
- License management
- Splunk apps
- Splunk configuration files
- Users, roles, and authentication
- Getting data in
- Distributed search
- Introduction to Splunk clusters
- Deploy forwarders with Forwarder Management
- Configure common Splunk data inputs
- Customize the input parsing process

Looking for more details? Review the test blueprint here.

Prerequisite Certification(s):

- Splunk Core Certified Power User
- Splunk Enterprise Certified Admin

Prerequisite Course(s):

- None

Recommended Next Steps:

- None

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> turn data into doing

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`

splunk> turn data into doing

Splunk Enterprise Security Certified Admin

What's on the Exam

This app-specific certification exam is an 57-minute, 61-question assessment which evaluates a candidate's knowledge and skills in the installation, configuration, and management of Splunk Enterprise Security. Candidates can expect an additional 3 minutes to review the exam agreement, for a total seat time of 60 minutes. It is recommended that candidates for this certification complete the lecture, hands-on labs, and quizzes that are part of the Administering Splunk Enterprise Security course, in order to be prepared for the certification exam.

The Administering Splunk Enterprise Security course focuses on Administrators who manage a Splunk Enterprise Security environment, including ES event processing and normalization, deployment requirements, technology add-ons, settings, risk analysis settings, threat intelligence and protocol intelligence configuration, and customizations.

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

- Identifying normal ES use cases
- Examining deployment requirements for typical ES installs
- Knowing how to install ES and gather information for lookups
- Knowing the steps to setting up inputs using technology add-ons
- Creating custom correlation searches
- Configuring ES risk analysis, threat, and protocol intelligence
- Fine tuning ES settings and other customizations

Looking for more details? Review the test blueprint here.

Prerequisite Certification(s):

- None

Prerequisite Course(s):

- None

Recommended Next Steps:

- Splunk Phantom Certified Admin

splunk> turn data into doing

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> turn data into doing

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> turn data into doing

Splunk IT Service Intelligence Certified Admin

What's on the Exam

This app-specific certification exam is a 57-minute, 53-question assessment which evaluates a candidate's knowledge and skills of the installation and configuration of Splunk's app for IT Service Intelligence (ITSI). Candidates can expect an additional 3 minutes to review the exam agreement, for a total seat time of 60 minutes. It is recommended that candidates for this certification complete the lecture, hands-on labs, and quizzes that are part of the Implementing IT Service Intelligence course in order to be prepared for the certification exam.

The Implementing ITSI course focuses on the use of ITSI to monitor mission-critical services. Major topics include ITSI architecture, deployment planning, installation, service design and implementation, configuring entities, notable events, and developing glass tables and deep dives.

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

- ITSI architecture and deployment
- Installing ITSI
- Designing Services - discovery and best practices
- Implementing services and entities
- Configuring correlation searches and multi KPI alerts
- Managing aggregation policies and anomaly detection
- Troubleshooting and maintenance

Looking for more details? Review the test blueprint here.

Prerequisite Certification(s):

- None

Prerequisite Course(s):

- None

Recommended Next Steps:

- None

splunk> turn data into doing

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> turn data into doing

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> turn data into doing

Splunk Phantom Certified Admin
What's on the Exam

This highly technical certification exam is a 57-minute, 58-question assessment which evaluates a candidate's knowledge and skills in installing and configuring a Phantom server and integrating it with Splunk, as well as planning, designing, creating, and debugging Playbooks. Candidates can expect an additional 3 minutes to review the exam agreement, for a total seat time of 60 minutes. It is recommended that candidates for this certification complete the lecture, hands-on labs, and quizzes that are part of the Administering Phantom, Developing Phantom Playbooks, and Advanced Phantom Implementation courses in order to be prepared for the certification exam.

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

- Installation/Initial configuration
- Apps and assets
- User management
- Ingesting data
- Events and containers
- Mission control
- Running actions and playbooks
- Case management/workflows
- Multi-tenacity
- Clustering
- Automation best practices
- The visual playbook editor
- Using actions and decisions
- Using action results
- Testing and debugging playbooks
- Using interaction
- Output formatting
- Complex logic
- Interacting with artifacts
- Using the vault in a playbook
- Custom lists
- Integrating Splunk with Phantom

Review the test blueprint here.

Prerequisite Certification(s):

- None

Prerequisite Course(s):

- None

Recommended Next Steps:

- None

splunk> turn data into doing