

# Splunk Certification

Certification Exam Study Guide

splunk®



# Splunk Certification

## Quick Link References



**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 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 Core Certified User](#)
- [Splunk Core Certified Power User](#)
- [Splunk Core Certified Advanced Power User](#)
- [Splunk Cloud Certified Admin](#)
- [Splunk Enterprise Certified Admin](#)
- [Splunk Enterprise Certified Architect](#)
- [Splunk Core Certified Consultant](#)
- [Splunk ES Certified Admin](#)
- [Splunk ITSI Certified Admin](#)
- [Splunk SOAR Certified Automation Developer](#)
- [Splunk O11y Cloud Certified Metrics User](#)
- [Splunk Certified Cybersecurity Defense Analyst](#)



**Prerequisite Certification(s):**

- None

**Prerequisite Course(s):**

- None

**Recommended Next Steps:**

- Splunk Core Certified Power User

# 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 the following courses:

- ☐ Intro to Splunk
- ☐ Using Fields
- ☐ Scheduling Reports and Alerts
- ☐ Visualizations
- ☐ Working with Time
- ☐ Statistical Processing
- ☐ Leveraging Lookups and Subsearches
- ☐ Search Optimization

Looking for more details? Review the test blueprint [here](#).

# 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`

**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 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 completing the following courses:

- ☐ Working with Time
- ☐ Statistical Processing
- ☐ Comparing Values
- ☐ Result Modification
- ☐ Correlation Analysis
- ☐ Creating Knowledge Objects
- ☐ Creating Field Extractions
- ☐ Data Models

Looking for more details? Review the test blueprint [here](#).

# 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



### Prerequisite Certification(s):

- Splunk Core Certified Power User

### Prerequisite Course(s):

- None

### Recommended Next Steps:

- Splunk Enterprise Certified Admin
- Splunk Cloud Certified Admin

# Splunk Core Certified Advanced Power User

## What's on the Exam?

This advanced certification exam is a 57-minute, 70-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 completed the following courses:

- ☐ Using Fields
- ☐ Working with Time
- ☐ Comparing Values
- ☐ Result Modification
- ☐ Leveraging Lookups and Subsearches
- ☐ Correlation Analysis
- ☐ Multivalue Fields
- ☐ Search Optimization
- ☐ Creating Knowledge Objects
- ☐ Creating Field Extractions
- ☐ Enriching Data with Lookups
- ☐ Data Models
- ☐ Introduction to Dashboards
- ☐ Dynamic Dashboards

Looking for more details? Review the test blueprint [here](#).

# Splunk Core Certified Advanced Power User

## Sample Questions

1. Where are transforming commands executed?
  - a. On indexers.
  - b. On search heads.
  - c. On forwarders.
  - d. It depends on their position in the search string.
  
2. At search time, Splunk creates tokens from event data. Where are they stored?
  - a. In a `journal.gz` file.
  - b. In a `props.conf` file.
  - c. In an `inputs.conf` file.
  - d. In a `.tsidx` file.
  
3. What is a default limitation of subsearches?
  - a. A subsearch returns no more than 10,000 events.
  - b. A subsearch must run in fewer than 30 seconds.
  - c. A subsearch can only be formatted with the `| return` command.
  - d. A subsearch only works by editing `limits.conf`.

# Splunk Core Certified Advanced Power User

## Answer Key

1. Where are transforming commands executed?
  - a. On indexers.
  - ☒ b. On search heads.
  - c. On forwarders.
  - d. It depends on their position in the search string.
  
2. At search time, Splunk creates tokens from event data. Where are they stored?
  - a. In a `journal.gz` file.
  - b. In a `props.conf` file.
  - c. In an `inputs.conf` file.
  - ☒ d. In a `.tsidx` file.
  
3. What is a default limitation of subsearches?
  - ☒ a. A subsearch returns no more than 10,000 events.
  - b. A subsearch must run in fewer than 30 seconds.
  - c. A subsearch can only be formatted with the `| return` command.
  - d. A subsearch only works by editing `limits.conf`.



#### Prerequisite Certification(s):

- Splunk Core Certified Power User

#### Prerequisite Course(s):

- None

#### Recommended Next Steps:

- Splunk ES Certified Admin
- Splunk ITSI Certified Admin
- Splunk SOAR Certified Automation Developer

## Splunk Cloud Certified Admin

### What's on the Exam?

This upper-level certification exam is a 72-minute, 60-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 Cloud Certified Admin

## Sample Questions

1. Which Windows input type collects data from the Windows OS logs?
  - a. Network
  - b. Performance
  - c. Event log
  - d. Host
  
2. If a new event's raw data contains a timestamp, what is the next check (or decision) that Splunk makes in the event timestamp processing logic?
  - a. Check if explicit time extraction rules exist in `props.conf`.
  - b. Check if the event contains a date.
  - c. Check if the file name contains a date.
  - d. Check if timestamps of nearby events from the same source are within a ten minute offset.
  
3. Which of the following is true about how users may be authenticated with Splunk Cloud?
  - a. Splunk native authentication, LDAP, and SAML authentication can all be used at the same time.
  - b. Splunk native authentication can be used with either LDAP or SAML authentication, but not both at the same time.
  - c. Enabling LDAP or SAML authentication disables Splunk native authentication.
  - d. Enabling Splunk native authentication disables LDAP and SAML authentication options.

# Splunk Cloud Certified Admin

## Answer Key

1. Which Windows input type collects data from the Windows OS logs?
  - a. Network
  - b. Performance
  - ☒ c. Event log
  - d. Host
  
2. If a new event's raw data contains a timestamp, what is the next check (or decision) that Splunk makes in the event timestamp processing logic?
  - ☒ a. Check if explicit time extraction rules exist in `props.conf`.
  - b. Check if the event contains a date.
  - c. Check if the file name contains a date.
  - d. Check if timestamps of nearby events from the same source are within a ten minute offset.
  
3. Which of the following is true about how users may be authenticated with Splunk Cloud?
  - a. Splunk native authentication, LDAP, and SAML authentication can all be used at the same time.
  - ☒ b. Splunk native authentication can be used with either LDAP or SAML authentication, but not both at the same time.
  - c. Enabling LDAP or SAML authentication disables Splunk native authentication.
  - d. Enabling Splunk native authentication disables LDAP and SAML authentication options.



### Prerequisite Certification(s):

- Splunk Core Certified Power User

### Prerequisite Course(s):

- None

### Recommended Next Steps:

- Splunk Enterprise Certified Architect
- Splunk ES Certified Admin
- Splunk ITSI Certified Admin
- Splunk SOAR Certified Automation Developer

## 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](#).



# 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)



### 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 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](#).

# 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 Core Certified Consultant



## Prerequisite Certification(s):

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

## Prerequisite Course(s):

- Core Consultant Labs
- Services: Core Implementation

## Recommended Next Steps:

- None

## 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):**

- None

**Prerequisite Course(s):**

- None

**Recommended Next Steps:**

- Splunk SOAR Certified Automation Developer

## Splunk Enterprise Security Certified Admin

### What's on the Exam?

This app-specific certification exam is an 57-minute, 48-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](#).

# 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`

**Prerequisite Certification(s):**

- None

**Prerequisite Course(s):**

- None

**Recommended Next Steps:**

- None

## 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](#).

# 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 SOAR Certified Automation Developer

## What's on the Exam?

This highly technical certification exam is a 57-minute, 45-question assessment which evaluates a candidate's knowledge and skills in installing and configuring a SOAR 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 Splunk SOAR*, *Investigating Splunk Incidents with SOAR*, *Developing SOAR Playbooks*, and *Advanced SOAR Implementation* courses in order to be prepared for the certification exam. *Formerly referred to as Splunk Phantom Certified Admin.*

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 SOAR (Phantom)

Review the test blueprint [here](#).



### Prerequisite Certification(s):

- None

### Prerequisite Course(s):

- None

### Recommended Next Steps:

- None



#### Prerequisite Certification(s):

- None

#### Prerequisite Course(s):

- None

#### Recommended Next Steps:

- Splunk Core Certified Power User
- Splunk SOAR Certified Automation Developer
- Splunk IT Service Intelligence Certified Administrator

## Splunk O11y Cloud Certified Metrics User

### What's on the Exam?

This foundational-level certification exam is a 60-minute, 54-question assessment which evaluates a candidate's knowledge and skills to skill sets in monitoring and investigating issues using Splunk Observability Cloud. This certification exam evaluates an individual's ability to monitor using built-in content, deploy and configure the OpenTelemetry Collector to send in metrics, visualize metrics, find insights using analytics, and set up alerts to monitor development environments in real time.

Splunk O11y Cloud Certified Metrics User is a recommended foundational-level certification track for all candidates in the observability/DevOps/SRE arena.

Candidates may reference the [Splunk How-To YouTube Channel](#), [Splunk Docs](#), and draw from their own Splunk experience. The following is a suggested and non-exhaustive list of training from our [Course Catalog](#) that may cover topics listed in the [exam blueprint](#):

- ☐ Getting Data into Splunk Observability Cloud
- ☐ Introduction to Splunk Observability
- ☐ Introduction to Splunk Infrastructure Monitoring
- ☐ Splunk Observability Cloud Teams
- ☐ Splunk Observability Cloud Enterprise Features
- ☐ Fundamentals of Metrics Monitoring in Splunk Observability
- ☐ Kubernetes Monitoring with Splunk Observability Cloud
- ☐ Visualizing and Alerting in Splunk Observability Cloud



### Prerequisite Certification(s):

- None - *it's recommended to have Power User Level Knowledge of Splunk Enterprise.*

### Prerequisite Course(s):

- None

### Recommended Next Steps:

- SOC administrator learning path
- Splunk Certified Cybersecurity Defense Engineer
- Splunk Enterprise Security Certified Admin

# Splunk Certified Cybersecurity Defense Analyst

## What's on the Exam?

This intermediate-level certification exam is a 75-minute, 66-question assessment which establishes a standard for users of Splunk Enterprise and Enterprise Security who wish to be certified as cybersecurity professionals. With this certification, you will be able to demonstrate knowledge critical to detecting, analyzing and combating cyber threats. Help protect businesses and mitigate risk, while managing vulnerabilities and threats using common types of cyber defense systems. Splunk Certified Cybersecurity Defense Analyst is a recommended certification track for all candidates in the cybersecurity/SOC analyst arena.

Candidates may reference the [Splunk How-To YouTube Channel](#), [Splunk Docs](#), [Splunk Boss of the SOC \(BOTS\) Blog](#), and draw from their own Splunk experience. The following is a suggested and non-exhaustive list of training from our [Course Catalog](#) that may cover topics listed in the [exam blueprint](#):

- ☐ The Cybersecurity Landscape
- ☐ Understanding Threats and Attacks
- ☐ Security Operations and the Defense Analyst
- ☐ Intro to Splunk
- ☐ Data and Tools for Defense Analysts
- ☐ Introduction to Enterprise Security
- ☐ Search under the hood
- ☐ The Art of investigation
- ☐ SOC Essentials: Investigating with Splunk ES
- ☐ SOC Essentials: Introduction to Threat Hunting
- ☐ Using Splunk Enterprise Security



### Prerequisite Certification(s):

- None - *it's recommended to have Power User Level Knowledge of Splunk Enterprise.*

### Prerequisite Course(s):

- None

### Recommended Next Steps:

- SOC administrator learning path
- Splunk Certified Cybersecurity Defense Analyst
- Splunk Enterprise Security Certified Admin

# Splunk Certified Cybersecurity Defense Engineer

## What's on the Exam?

This professional-level certification exam is a 75-minute, 60-question assessment which establishes an intermediate-level standard for users of Splunk Enterprise, Enterprise Security, and Splunk SOAR who wish to be certified as cybersecurity professionals. With this certification, you will be able to demonstrate knowledge critical to optimizing detection and automation in a SOC environment. Splunk Certified Cybersecurity Defense Engineer is a recommended certification track for all candidates in the cybersecurity/SOC defense engineer arena.

Candidates may reference the [Splunk How-To YouTube Channel](#), [Splunk Docs](#), Splunk Blogs especially [Splunk Threat Research Team \(STRT\)](#), [Splunk Boss of the SOC \(BOTS\) Blog](#), and draw from their own Splunk experience. In addition to the courses listed for Splunk Certified Cybersecurity Defense Analyst, the following is a suggested and non-exhaustive list of training from our [Course Catalog](#) that may cover topics listed in the [exam blueprint](#):

- ☐ Using Splunk Enterprise Security
- ☐ Developing SOAR Playbooks
- ☐ Introduction to Splunk Security Essentials
- ☐ Administering Splunk Enterprise Security
- ☐ Splunk Enterprise Data Administration