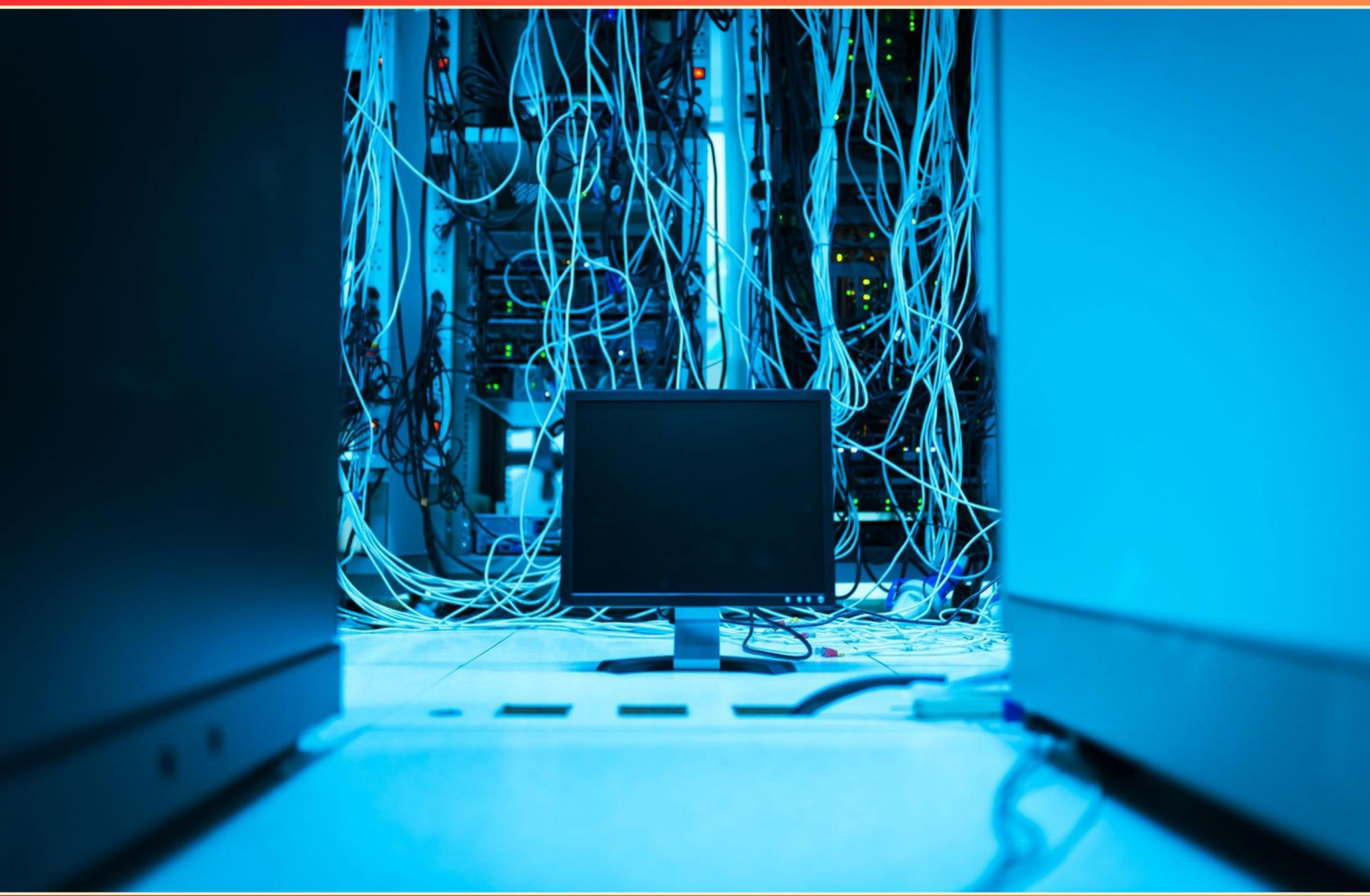
SPLUNK ENTERPRISE CERTIFIED ADMIN PRACTICE TEST (SAMPLE)

STUDY GUIDE



SAMPLE STUDY GUIDE WITH LIMITED QUESTIONS

VISIT US ONLINE FOR THE FULL VERSION STUDY GUIDE

https://splunkcertifiedadmin.examzify.com

Table of Contents

Introduction

Preparing for a certification exam can feel overwhelming, but with the right tools, it becomes an opportunity to build confidence, sharpen your skills, and move one step closer to your goals. At Examzify, we believe that effective exam preparation isn't just about memorization, it's about understanding the material, identifying knowledge gaps, and building the test-taking strategies that lead to success.

This guide was designed to help you do exactly that.

Whether you're preparing for a licensing exam, professional certification, or entry-level qualification, this book offers structured practice to reinforce key concepts. You'll find a wide range of multiple-choice questions, each followed by clear explanations to help you understand not just the right answer, but why it's correct.

The content in this guide is based on real-world exam objectives and aligned with the types of questions and topics commonly found on official tests. It's ideal for learners who want to:

- Practice answering questions under realistic conditions,
- Improve accuracy and speed,
- Review explanations to strengthen weak areas, and
- Approach the exam with greater confidence.

We recommend using this book not as a stand-alone study tool, but alongside other resources like flashcards, textbooks, or hands-on training. For best results, we recommend working through each question, reflecting on the explanation provided, and revisiting the topics that challenge you most.

Remember: successful test preparation isn't about getting every question right the first time, it's about learning from your mistakes and improving over time. Stay focused, trust the process, and know that every page you turn brings you closer to success.

Let's begin.

How to Use This Guide

This guide is designed to help you study more effectively and approach your exam with confidence. Whether you're reviewing for the first time or doing a final refresh, here's how to get the most out of your Examzify study guide:

1. Start with a Diagnostic Review

Skim through the questions to get a sense of what you know and what you need to focus on. Your goal is to identify knowledge gaps early.

2. Study in Short, Focused Sessions

Break your study time into manageable blocks (e.g. 30 – 45 minutes). Review a handful of questions, reflect on the explanations.

3. Learn from the Explanations

After answering a question, always read the explanation, even if you got it right. It reinforces key points, corrects misunderstandings, and teaches subtle distinctions between similar answers.

4. Track Your Progress

Use bookmarks or notes (if reading digitally) to mark difficult questions. Revisit these regularly and track improvements over time.

5. Simulate the Real Exam

Once you're comfortable, try taking a full set of questions without pausing. Set a timer and simulate test-day conditions to build confidence and time management skills.

6. Repeat and Review

Don't just study once, repetition builds retention. Re-attempt questions after a few days and revisit explanations to reinforce learning. Pair this guide with other Examzify tools like flashcards, and digital practice tests to strengthen your preparation across formats.

There's no single right way to study, but consistent, thoughtful effort always wins. Use this guide flexibly, adapt the tips above to fit your pace and learning style. You've got this!

Questions

1. **When adding a Search Peer in Splunk, which capability must the user account possess?**

   A. Edit_roles

   B. Edit_user

   C. Admin

   D. Search

2. **What are the levels of permissions for knowledge objects in Splunk?**

   A. Private

   B. Shared in App

   C. All apps (Global)

   D. All of the above

3. **Which of the following is not considered remote data?**

   A. A universal forwarder forwards data to a search head/indexer combination

   B. A forwarder forwards data to an indexer cluster which then forwards data to a search head cluster

   C. A forwarder forwards data to another forwarder, which forwards data to a search head/indexer combination

   D. With a search head/indexer combination, we monitor files and directories on the machine on which Splunk Enterprise is installed

4. **Are compressed gzip files automatically handled by the file monitor input?**

   A. Yes, they are unzipped before ingestion

   B. No, they need to be extracted manually

   C. Yes, but only if specified

   D. No, it does not support gzip files

5. **In which bucket does the most "live" data exist?**

   A. Warm

   B. Cold

   C. Hot

   D. Thawed

6. Which configuration is indexed third at index time in Splunk?

A. App local directories

B. App default directories

C. System default directories

D. Etc/system/local

7. What is preferable to deleting an app?

A. Disabling the app

B. Moving the app's files to another location

C. Reinstalling the app later

D. Both disabling and moving the app's files

8. True or False: Event Boundaries can be defined using props.conf at the Universal forwarder level.

A. True

B. False

C. Only at the indexer level

D. Only at the Heavy Forwarder level

9. Which default host field does NOT pertain to the Connection_Host configuration?

A. DNS

B. IP

C. MAC Address

D. None

10. How are configuration files merged within Splunk?

A. Only the first loaded file is used

B. All inputs.conf files are merged into one master configuration

C. Files are ignored if they have identical settings

D. Only default configurations apply at runtime

Answers

1. B
2. D
3. D
4. A
5. C
6. B
7. D
8. A
9. C
10. B

Explanations

1. When adding a Search Peer in Splunk, which capability must the user account possess?

A. Edit_roles

B. Edit_user

C. Admin

D. Search

To add a Search Peer in Splunk, a user account must possess the capability to edit user settings, which is inherent in the capability of editing roles or user accounts. This capability allows the account to manage user settings and configurations within the Splunk environment, including the ability to add new search peers. Having the ability to edit users or roles is critical since adding a search peer can involve adjusting configurations that are associated with user roles and permissions. Without this capability, a user would be restricted from making the necessary changes or additions to the search infrastructure. The other capabilities, while important in different contexts within Splunk's operations, do not specifically provide the necessary permissions needed to manage search peer configurations. The Admin capability includes a broader range of permissions but is not as directly relevant in the context of adding a search peer, focusing instead on overall system administration. Similarly, the Search capability simply allows users to execute searches and does not grant permissions for managing system settings.

2. What are the levels of permissions for knowledge objects in Splunk?

A. Private

B. Shared in App

C. All apps (Global)

D. All of the above

In Splunk, knowledge objects such as saved searches, event types, and field aliases, have varying levels of permissions that dictate accessibility and sharing among users. Understanding these levels is crucial for managing access to data and configurations effectively. The three identified levels of permissions—Private, Shared in App, and All apps (Global)—represent different scopes of access: - The Private level allows knowledge objects to be accessible only to the user who created them. This means that other users cannot see or use these objects unless explicitly shared. - Shared in App refers to knowledge objects that are accessible to all users who have access to the specific application where the objects reside. This is useful for collaborative environments where multiple users working within the same app need access to shared resources. - The All apps (Global) level signifies that the knowledge object is available across all applications. This grants the widest scope of access, allowing any user, regardless of the app context, to utilize the object. Since all three options accurately describe specific and distinct levels of permissions for knowledge objects in Splunk, the correct answer encompasses all these possibilities, confirming that D, which includes all mentioned levels of permissions, is the most comprehensive and accurate choice. Understanding this framework aids in effectively controlling user access and maintaining data

3. Which of the following is not considered remote data?

A. A universal forwarder forwards data to a search head/indexer combination

B. A forwarder forwards data to an indexer cluster which then forwards data to a search head cluster

C. A forwarder forwards data to another forwarder, which forwards data to a search head/indexer combination

D. With a search head/indexer combination, we monitor files and directories on the machine on which Splunk Enterprise is installed

The correct choice identifies the scenario where data is being accessed and processed locally, rather than remotely. When using a search head and indexer combination, monitoring files and directories on the machine where Splunk Enterprise is installed means that the data is directly on the local filesystem. Since this data is being processed on the same system, it does not fall under the category of remote data. In contrast, the other scenarios involve data that is sourced from different locations. Forwarders transmit data either to an indexer cluster or to another forwarder, both of which imply the movement of data from one system to another, representative of a remote data operation. These setups are designed to facilitate data collection from various sources that are not on the Splunk instance itself, allowing for scalable data management across multiple systems. Thus, option D accurately highlights the local nature of the data being monitored, differentiating it from the remote data scenarios described in the other choices.

4. Are compressed gzip files automatically handled by the file monitor input?

A. Yes, they are unzipped before ingestion

B. No, they need to be extracted manually

C. Yes, but only if specified

D. No, it does not support gzip files

When using the file monitor input in Splunk, compressed gzip files are indeed automatically handled and unzipped before ingestion. This capability allows Splunk to natively process gzip files, streamlining data ingestion by eliminating the need for manual extraction of the compressed data. This feature is particularly beneficial as it simplifies data management and ensures that users can work with the most current data without having to take additional steps to uncompress files prior to ingestion. The automatic handling of gzip files is part of Splunk's design to efficiently manage data input from various sources, improving usability and reducing administrative overhead. Thus, the choice indicating that gzip files are automatically unzipped before ingestion accurately reflects Splunk's built-in functionality for handling such compressed formats.

5. In which bucket does the most "live" data exist?

A. Warm

B. Cold

C. Hot

D. Thawed

The bucket that contains the most "live" data is the hot bucket. In Splunk, data is categorized into different types of buckets based on its age and the frequency of access. This classification is essential for efficient data management and system performance. The hot bucket is where newly ingested data is immediately stored. It is the first stop for incoming data, making it the most actively used and frequently accessed. Data in hot buckets is often being written to or modified and is readily available for real-time searches. As data ages and becomes less frequently accessed, it is eventually moved into a warm bucket and, later, into cold and thawed buckets, which are used less frequently. Therefore, since hot buckets represent the most current data being actively engaged with, they rightly contain the most "live" data in the Splunk environment.

6. Which configuration is indexed third at index time in Splunk?

A. App local directories

B. App default directories

C. System default directories

D. Etc/system/local

In Splunk, the order of how configurations are indexed at index time is determined by a hierarchy that Splunk follows to manage various settings across different contexts. Indexed third at index time refers to the application of configurations from the app default directories. The app default directories are part of the hierarchy where default configurations for apps are stored. They are loaded after the system default settings but before app local settings. This means that if a configuration is specified in the app default directories, it can be overridden by configurations in the app local directories, which are considered after the app defaults. Understanding this order is crucial for managing Splunk's behavior, especially when you are applying configurations that need to maintain specific priorities or properties in the data processing pipeline. The distinction ensures that custom settings are respected and prioritized over default settings, allowing for flexibility and customization in how Splunk interacts with data.

7. What is preferable to deleting an app?

A. Disabling the app

B. Moving the app's files to another location

C. Reinstalling the app later

D. Both disabling and moving the app's files

Disabling the app is generally preferable to deleting it as it allows the configuration and settings to remain intact while preventing the app from running. This is useful in situations where the app might be needed again in the future, as it can easily be re-enabled without requiring a complete reinstallation or configuration adjustment. On the other hand, moving the app's files can also be beneficial in certain cases. It allows for a temporary removal of the app while keeping its files secure in case it needs to be restored or inspected later. Moving the files out of the application directory ensures that they won't interfere with other applications or the overall system. Both of these actions serve to maintain system integrity and ease of management. Disabling the app ensures it won't process any data or impact performance while still allowing for quick reinstatement, while moving files provides a layer of safety for the app's components. This combination of actions allows for flexibility and control in managing applications within Splunk, making it clear why choosing both options is viewed as preferable.

8. True or False: Event Boundaries can be defined using props.conf at the Universal forwarder level.

A. True

B. False

C. Only at the indexer level

D. Only at the Heavy Forwarder level

The statement is true because event boundaries can indeed be defined using the props.conf at the Universal Forwarder level in Splunk. The Universal Forwarder processes the data it collects and applies the configurations specified in props.conf to determine how to handle the events before they are sent to the indexers. This configuration includes setting event boundaries, which defines how to segment incoming raw data into distinct events. Defining event boundaries at the Universal Forwarder level allows for initial parsing to occur as close to the data source as possible, optimizing performance and ensuring that the data is structured correctly before it reaches the indexers for storage and further analysis. This capability is critical for managing data effectively in a Splunk deployment, and it supports the overall architecture by allowing for early handling of event segmentation based on the specific needs of the data source. Other options are limited in different ways; for instance, event boundaries could also be defined on Heavy Forwarders and Indexers, but they are not exclusively defined there—meaning that all levels (including the Universal Forwarder) can handle these settings.

9. Which default host field does NOT pertain to the Connection_Host configuration?

A. DNS

B. IP

C. MAC Address

D. None

The Connection_Host configuration in Splunk primarily determines how the host field is extracted from incoming data. The default options for this configuration include using the DNS name of the host and the IP address of the machine generating the logs, as these readily provide a means of identifying the source of the data. In contrast, the MAC Address does not factor into the Connection_Host configuration. The MAC Address is specific to network hardware and does not serve the same purpose in the context of identifying data sources in Splunk's indexing framework. It is less relevant for log management and is not typically featured in the host identification processes inherent to most logging and data collection methods. Thus, the correct choice is the MAC Address since it is not utilized by the Connection_Host configuration in Splunk.

10. How are configuration files merged within Splunk?

A. Only the first loaded file is used

B. All inputs.conf files are merged into one master configuration

C. Files are ignored if they have identical settings

D. Only default configurations apply at runtime

When it comes to how configuration files are merged within Splunk, it's important to understand the design and functionality of the configuration management system. Splunk is built to allow for flexibility and extensibility through its configuration files, which include files like inputs.conf, props.conf, and many others. The process of merging configuration files occurs in a way that allows all relevant configurations to be combined into one master configuration. This means that if there are multiple inputs.conf files located in various directories or from different apps, they will not simply be overridden by the first loaded file. Instead, all configurations from these separate inputs.conf files are merged together, which means that in scenarios where different files have the same setting, later configurations can take precedence based on the order of loading. This merging behavior comes from Splunk's hierarchical configuration system, which allows users to customize settings across different layers, such as default configurations, local configurations, and various apps. Thus, the merging of all inputs.conf files into one master configuration is crucial for achieving the desired data ingestion and processing without being limited by the constraints of having a single configuration file. This merging strategy enables interface flexibility and promotes efficient configuration management, making it easier for administrators to manage complex environments with numerous data inputs.

Next Steps

Congratulations on reaching the final section of this guide. You've taken a meaningful step toward passing your certification exam and advancing your career.

As you continue preparing, remember that consistent practice, review, and self-reflection are key to success. Make time to revisit difficult topics, simulate exam conditions, and track your progress along the way.

If you need help, have suggestions, or want to share feedback, we'd love to hear from you. Reach out to our team at hello@examzify.com.

Or visit your dedicated course page for more study tools and resources:

https://splunkcertifiedadmin.examzify.com

We wish you the very best on your exam journey. You've got this!