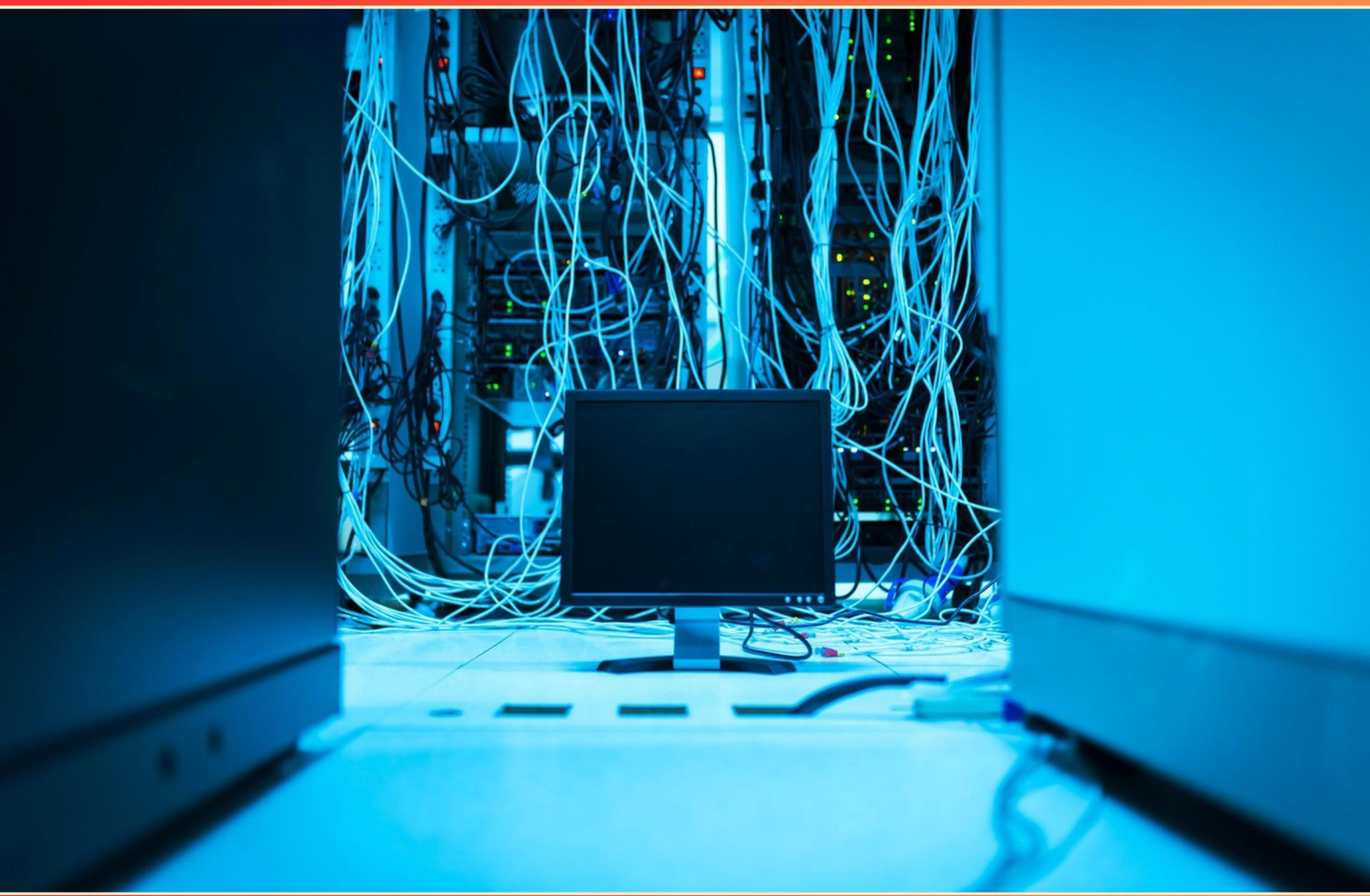
SPLUNK ENTERPRISE CERTIFIED ADMIN PRACTICE TEST (SAMPLE)

STUDY GUIDE



SAMPLE STUDY GUIDE WITH LIMITED QUESTIONS

VISIT US ONLINE FOR THE FULL VERSION STUDY GUIDE

https://splunkcertifiedadmin.examzify.com

Copyright © 2026 by Examzify - A Kaluba Technologies Inc. product.

ALL RIGHTS RESERVED.

No part of this book may be reproduced or transferred in any form or by any means, graphic, electronic, or mechanical, including photocopying, recording, web distribution, taping, or by any information storage retrieval system, without the written permission of the author.

Notice: Examzify makes every reasonable effort to obtain accurate, complete, and timely information about this product from reliable sources.

SAMPLE

Table of Contents

Copyright 1

Table of Contents 2

Introduction 3

How to Use This Guide 4

Questions 5

Answers 8

Explanations 10

Next Steps 16

SAMPLE

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.

SAMPLE

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!

SAMPLE

Questions

SAMPLE

1. How can forwarders specify SSL settings for secure connections?

A. In inputs.conf file

B. In outputs.conf file

C. In props.conf file

D. In server.conf file

2. What configuration file would you edit to set up SSL for Splunk inputs?

A. props.conf

B. inputs.conf

C. outputs.conf

D. server.conf

3. Which command is used to recursively search through directories and subdirectories for a match?

A. Wildcard

B. Ellipsis (...)

C. Recursive Search

D. Directory Search

4. Is the statement true or false? Time extraction can be done using props.conf on the UF and HF.

A. True

B. False

C. Depends on configuration

D. Only on HF

5. Can StatsD data be used to collect metric data using HTTPS and HEC?

A. True

B. False

C. Only for specific applications

D. Only in experimental setups

SAMPLE

6. What is the primary function of the Splunk indexer?

A. To collect data from various sources

B. To store and retrieve indexed data

C. To visualize data

D. To manage user access

7. What type of data does the KV Store work with in Splunk?

A. Binary data

B. Text logs only

C. Key-value pairs

D. Structured data only

8. Which stanzas are typically included in outputs.conf for forwarding data?

A. TCP_INPUT and TCP_OUTPUT

B. HTTP_EVENT and HTTP_OUTPUT

C. TCPOUT and HTTP

D. TCP_INPUT and HTTP

9. What is the function of a Heavy Forwarder in a Splunk environment?

A. To search indexed data

B. To forward data to indexers

C. To monitor data inputs

D. To manage user access

10. What are the four default metadata items in Splunk?

A. source, host, sourcetype, index

B. source, port, sourcetype, index

C. host, indexer, sourcetype, data

D. host, source, app, index

SAMPLE

Answers

SAMPLE

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

SAMPLE

Explanations

SAMPLE

1. How can forwarders specify SSL settings for secure connections?

A. In inputs.conf file

B. In outputs.conf file

C. In props.conf file

D. In server.conf file

The ability of forwarders to specify SSL settings for secure connections is indeed done in the outputs.conf file. This file is crucial for configuring how data is sent from forwarders to indexers, including the secure transport protocols that should be employed. In outputs.conf, administrators can define parameters such as `useClientSSL`, `clientSSLConfig`, and others that directly relate to SSL configurations. By setting these parameters, forwarders can enforce encrypted communication to ensure data is securely transmitted over the network, protecting against eavesdropping and tampering. The inputs.conf file deals mainly with the data that the forwarder collects, such as setting up inputs and processing data, so it does not control how that data is sent. The props.conf file is used for data transformation and does not manage the transport security aspects, while the server.conf file primarily relates to server-specific settings, including general configurations on how Splunk operates, but it isn't specifically for SSL settings in the context of forwarding data. Thus, specifying SSL settings is inherently tied to the outputs.conf file, making it the correct choice for this scenario.

2. What configuration file would you edit to set up SSL for Splunk inputs?

A. props.conf

B. inputs.conf

C. outputs.conf

D. server.conf

The correct configuration file to edit for setting up SSL for Splunk inputs is inputs.conf. This file is specifically designed for configuring data inputs, which includes the settings for how data is collected into Splunk. When establishing secure connections for inputs, such as those for receiving data over HTTPS or SSL-encrypted protocols, the necessary parameters (like SSL certificates and private key locations) are configured within inputs.conf. Each of the other configuration files mentioned serves different purposes in the Splunk architecture. For example, props.conf is used for defining how Splunk processes incoming data, including parsing and indexing attributes, but it does not handle network security settings. Outputs.conf deals with the forwarding configuration for sending data to other Splunk instances and is not related to input data security. Server.conf contains general server configuration settings and defines server roles, but it also does not focus on the specifics of input data or SSL settings. Thus, when it comes to setting up SSL for data inputs in Splunk, inputs.conf is the relevant file where these configurations must be specified.

SAMPLE

3. Which command is used to recursively search through directories and subdirectories for a match?

A. Wildcard

B. Ellipsis (...)

C. Recursive Search

D. Directory Search

The choice of ellipsis (...) as the answer indicates a specific syntax that often represents recursion in various programming and command-line contexts. In many systems, ellipsis can symbolize an operation that acts on all levels or tiers beneath a given point in a directory structure. This is especially relevant in searching contexts, where recursion implies going beyond the initial directory to include all nested directories and files. In Splunk's context, while the exact terminology might differ, the essence of recursive searching indicates a process where the command must inherently understand and navigate through a hierarchy of directories. By using ellipsis, it suggests an inclusive approach to searching, capturing all potential matches across multiple levels of data. The other options do not even closely reflect the nature of recursive searching. Wildcards are typically used for pattern matching within file names but do not indicate a hierarchical search across directories. Directory search is a broad term and lacks specificity about the nature of the recursive operation, while recursive search, although closely related conceptually, is not characterized by a specific command structure such as the ellipsis. This provides clarity in the context of command-line usage where succinct symbols convey more precise operational meaning, particularly in recursion scenarios.

4. Is the statement true or false? Time extraction can be done using props.conf on the UF and HF.

A. True

B. False

C. Depends on configuration

D. Only on HF

The statement regarding time extraction in relation to props.conf requires a nuanced understanding of where time extraction configurations can be applied in the Splunk environment. Time extraction is primarily handled at the Heavy Forwarder (HF) and Indexer layers, not the Universal Forwarder (UF). The Universal Forwarder is designed to be a lightweight agent that collects and forwards logs without performing significant processing. As such, it does not process props.conf for time extraction purposes. Time extraction configurations, including parsing and field extractions, are typically executed on the Heavy Forwarder or Indexers where full data processing capabilities are available. This makes the assertion false, as time extraction cannot be configured directly on the Universal Forwarder using props.conf. Instead, all necessary configurations for parsing and field extraction, including time, should be done at the Heavy Forwarder or Indexer levels where Splunk can effectively apply these settings to the incoming data.

SAMPLE

5. Can StatsD data be used to collect metric data using HTTPS and HEC?

A. True

B. False

C. Only for specific applications

D. Only in experimental setups

StatsD is a network daemon that listens for statistics, like counters and timers, sent over UDP or TCP, and it aggregates these statistics and sends them to graphing and monitoring platforms. In the context of using StatsD data to collect metric data in Splunk, the HTTP Event Collector (HEC) is designed to ingest event data via HTTPS. The correct understanding here is that StatsD does not natively support transmission of data over HTTPS or integration with HEC directly. Instead, StatsD typically sends data using UDP or TCP protocols, which means that this choice is more aligned with traditional data collection methods rather than using HEC over HTTPS. While there may be workarounds or third-party tools that could facilitate StatsD data collection in this manner, as per its standard operations and in accordance with Splunk's ingestion capabilities, the premise is that StatsD data can't be directly utilized in conjunction with HTTPS and HEC without some intermediary or additional configuration. Hence, the statement is accurately determined to be false.

6. What is the primary function of the Splunk indexer?

A. To collect data from various sources

B. To store and retrieve indexed data

C. To visualize data

D. To manage user access

The primary function of the Splunk indexer is to store and retrieve indexed data. In Splunk, indexing is the process of taking raw machine data, parsing it, and then storing it in a way that optimizes it for fast querying and retrieval. This allows users to efficiently search for and analyze the data later. Once the raw data is ingested, the indexer creates an index, which is essentially a data structure that enables quick access to the specific data, even when dealing with large volumes of information. The indexer also handles data compression and storage management, ensuring that the indexed data is stored efficiently and can be retrieved quickly when needed. The other options relate to different functions within Splunk: collecting data is typically done by forwarders, visualizing data involves the use of dashboards and charts in the Splunk interface, and managing user access concerns user roles and permissions, which is handled through Splunk's access control features. These functions are essential in their own right, but they do not encompass the core purpose of the indexer within the Splunk architecture.

SAMPLE

7. What type of data does the KV Store work with in Splunk?

A. Binary data

B. Text logs only

C. Key-value pairs

D. Structured data only

The KV Store in Splunk is designed specifically to work with key-value pairs. This functionality allows users to store, retrieve, and manage data in a way that is structured as key-value pairs, which is a common format for efficiently organizing and accessing information. The KV Store enables users to leverage NoSQL database capabilities directly within the Splunk environment, facilitating advanced use cases such as data lookups and faster query handling. Key-value pairs provide a flexible way to organize data since each piece of information can be accessed using a unique key, making it easy to retrieve specific data based on its corresponding value. This is particularly helpful for use cases that involve dynamic datasets where data relationships and structures might change frequently. The other types of data mentioned do not precisely fit the KV Store's purpose. For example, while the KV Store could store structured data, it is not limited to that form and is not designed exclusively for structured data or binary data. It also accommodates a broader range than just text logs, reinforcing its versatility in handling various forms of key-value pair data.

8. Which stanzas are typically included in outputs.conf for forwarding data?

A. TCP_INPUT and TCP_OUTPUT

B. HTTP_EVENT and HTTP_OUTPUT

C. TCPOUT and HTTP

D. TCP_INPUT and HTTP

The inclusion of TCPOUT and HTTP stanzas in the outputs.conf file is essential for configuring data forwarding in Splunk. The TCPOUT stanza is specifically designed for configuring the settings related to forwarding data over TCP to one or more indexers. This allows for streamlined, efficient transmission of log data, which is vital in a distributed data architecture. By defining the target indexers, port numbers, and additional settings, users can effectively manage how and where their data will be sent. Moreover, the HTTP stanza can be included to enable the forwarding of data that is ingested via HTTP or HTTPS. This is particularly useful when integrating with services that send data to Splunk over web protocols, making it versatile for different data sources. By including these two types of stanzas, you ensure comprehensive configuration for forwarding both TCP and HTTP events, which are common use cases in many Splunk environments. Other options do not accurately reflect the standard configuration practices in outputs.conf. For instance, the mentioned stanzas in options involving TCP_INPUT or HTTP_EVENT are not typically associated with outputs.conf since they pertain to data input configurations rather than output or forwarding configurations. Using the correct stanzas ensures the data forwarding behaves as expected, leading to a well-functioning Spl

SAMPLE

9. What is the function of a Heavy Forwarder in a Splunk environment?

A. To search indexed data

B. To forward data to indexers

C. To monitor data inputs

D. To manage user access

The function of a Heavy Forwarder in a Splunk environment is to forward data to indexers. A Heavy Forwarder is designed to handle both data collection and data forwarding with a high level of processing capability. It can perform parsing and indexing before forwarding, allowing for the efficient transfer of data to Splunk indexers. This capability enables it to filter, transform, and route data based on specific configurations, ensuring that the right data reaches the indexers in a timely manner. While other components of a Splunk deployment have their specific roles, such as monitoring data inputs or managing user access, the Heavy Forwarder is uniquely focused on the data forwarding process. It excels in environments where data needs to be processed before it's sent to the indexers, allowing for more efficient resource utilization and better data management.

10. What are the four default metadata items in Splunk?

A. source, host, sourcetype, index

B. source, port, sourcetype, index

C. host, indexer, sourcetype, data

D. host, source, app, index

*The four default metadata items in Splunk are indeed source, host, sourcetype, and index. These elements play crucial roles in how data is ingested, organized, and searchable within the Splunk platform. - **Source** refers to the origin of the data, helping to identify where the information comes from. This could be a file path, URL, or specific device that generates the log data. Understanding the source helps in auditing and tracing back the events. - **Host** indicates the machine or environment from which the data originates. This is particularly useful when monitoring in complex environments where multiple hosts may generate similar data. Being able to identify the host allows for more targeted searches and monitoring. - **Sourcetype** provides a mechanism to classify the nature of the data being ingested. It tells Splunk how to parse and interpret the incoming data, which is vital for accurate indexing and for applying the right extraction rules to the data. - **Index** is where the data is stored in Splunk, serving as a key organizational structure. Each index can be configured separately, allowing for optimization in performance, storage, and data retrieval. These four metadata items not only help in indexing and searching the data more effectively but also aid in*

SAMPLE

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!

SAMPLE