

Splunk

Exam Questions SPLK-1005

Splunk Cloud Certified Admin



NEW QUESTION 1

What are the four default roles that Splunk Cloud Platform comes with?

- A. admin, power, user, can_delete
- B. admin, power, user, sc_admin
- C. admin, power, user, guest
- D. admin, power, user, can_write

Answer: B

NEW QUESTION 2

Which option in Splunk Web can be used to create a new local TCP input?

- A. Settings > Data Inputs > TCP > New Local TCP
- B. Settings > Data Inputs > TCP > Add New
- C. Settings > Data Inputs > TCP > Create New
- D. Settings > Data Inputs > TCP > New Data Input

Answer: A

NEW QUESTION 3

Which option in Splunk web can be used to access the Guided Data On-boarding feature?

- A. Add data
- B. Data inputs
- C. Data summary
- D. Data models

Answer: A

NEW QUESTION 4

Which command can be used to run a 'splunk diag' on both the indexer and the forwarder?

- A. splunk diag -collect all -uri https://<username>:<password>@<host>:<port>
- B. splunk diag -collect all -auth <username>:<password>
- C. splunk diag -collect all -server <host>:<port>
- D. splunk diag -collect all -user <username> -password <password>

Answer: B

NEW QUESTION 5

What is the name of the Splunk Cloud setting that allows you to specify the maximum amount of raw data allowed before data is removed from the index?

- A. Max raw data size
- B. Max data retention
- C. Max index size
- D. Max data volume

Answer: A

NEW QUESTION 6

What is the name of the process that breaks the stream of raw data into individual lines called events?

- A. Line breaking
- B. Event annotation
- C. Event transformation
- D. Timestamp extraction

Answer: A

NEW QUESTION 7

Which tool can be used to verify that data is actually being received on the specified port on the indexing server?

- A. tcpdump
- B. netstat
- C. ping
- D. traceroute

Answer: A

NEW QUESTION 8

Which setting in inputs.conf can be used to specify the maximum size of a file that can be monitored by Splunk?

- A. max_file_size
- B. max_file_age
- C. max_file_count
- D. max_file_bytes

Answer: A

NEW QUESTION 9

What is the main difference between events indexes and metrics indexes in Splunk Cloud?

- A. Events indexes impose minimal structure and can accommodate any kind of data, while metrics indexes use a highly structured format to handle metrics data.
- B. Events indexes use a highly structured format to handle event-based log data, while metrics indexes impose minimal structure and can accommodate any kind of data.
- C. Events indexes store data in compressed form, while metrics indexes store data in uncompressed form.
- D. Events indexes store data in uncompressed form, while metrics indexes store data in compressed form.

Answer: A

NEW QUESTION 10

Which setting in inputs.conf can be used to set the host field to a static value for a monitor input?

- A. host
- B. host_regex
- C. host_segment
- D. host_override

Answer: A

NEW QUESTION 10

Which configuration file contains the settings for event line breaking and line merging?

- A. inputs.conf
- B. outputs.conf
- C. props.conf
- D. transforms.conf

Answer: C

NEW QUESTION 13

What is the name of the Splunk Cloud feature that allows you to get data from APIs and other remote data interfaces through scripted inputs?

- A. Splunk Cloud Data Connectors
- B. Splunk Cloud Data Integrations
- C. Splunk Cloud Data Collectors
- D. Splunk Cloud Data Sources

Answer: C

NEW QUESTION 14

Which type of forwarder can perform data parsing and enrichment before sending it to the indexer?

- A. Universal forwarder
- B. Heavy forwarder
- C. Deployment server
- D. Search head

Answer: B

NEW QUESTION 17

What is the name of the configuration file that governs data inputs such as forwarders and file system monitoring?

- A. inputs.conf
- B. props.conf
- C. transforms.conf
- D. outputs.conf

Answer: A

NEW QUESTION 19

What is the name of the component that acts as a data manager and sends data to Splunk Cloud Platform indexers?

- A. Heavy forwarder
- B. Universal forwarder
- C. Deployment server
- D. License master

Answer: A

NEW QUESTION 21

Which option can be used to specify the host value of the data when creating a file or directory monitor input?

- A. Set Host
- B. Select Host
- C. Choose Host
- D. Define Host

Answer: A

NEW QUESTION 25

What is the name of the topology that allows you to initiate searches from an on-premises Splunk Enterprise search head to a single Splunk Cloud Platform deployment?

- A. Hybrid Search Topology
- B. Federated Search Topology
- C. Distributed Search Topology
- D. Clustered Search Topology

Answer: A

NEW QUESTION 28

What is the name of the first step that you need to perform to configure the LDAP authentication scheme with Splunk Web?

- A. Create an LDAP strategy
- B. Map LDAP groups to Splunk roles
- C. Configure LDAP settings
- D. Test LDAP connection

Answer: A

NEW QUESTION 30

Which setting in inputs.conf can be used to specify the SSL certificate for a TCP or UDP input?

- A. sslCertPath
- B. sslRootCAPath
- C. sslPassword
- D. All of the above

Answer: D

NEW QUESTION 32

.....

Thank You for Trying Our Product

We offer two products:

1st - We have Practice Tests Software with Actual Exam Questions

2nd - Questions and Answers in PDF Format

SPLK-1005 Practice Exam Features:

- * SPLK-1005 Questions and Answers Updated Frequently
- * SPLK-1005 Practice Questions Verified by Expert Senior Certified Staff
- * SPLK-1005 Most Realistic Questions that Guarantee you a Pass on Your FirstTry
- * SPLK-1005 Practice Test Questions in Multiple Choice Formats and Updatesfor 1 Year

100% Actual & Verified — Instant Download, Please Click
[Order The SPLK-1005 Practice Test Here](#)