

Splunk

Exam Questions SPLK-1005

Splunk Cloud Certified Admin



NEW QUESTION 1

What is the name of the attribute that you need to set to true in the [search] stanza of the limits.conf file to enable Data Preview?

- A. timeline_events_preview
- B. data_preview_enabled
- C. show_data_preview
- D. enable_data_preview

Answer: A

NEW QUESTION 2

Which feature of forwarders can protect the data from unauthorized access or tampering?

- A. Data compression
- B. SSL security
- C. Data masking
- D. Data encryption

Answer: B

NEW QUESTION 3

Which configuration file needs to be edited to enable local indexing on the forwarder?

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

Answer: A

NEW QUESTION 4

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

- A. Set Source Type
- B. Select Source Type
- C. Choose Source Type
- D. Define Source Type

Answer: A

NEW QUESTION 5

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 6

What is the name of the default field that stores the timestamps in UNIX time when data is indexed?

- A. _time
- B. _timestamp
- C. _date
- D. _epoch

Answer: A

NEW QUESTION 7

Which network protocol is recommended for sending data to Splunk because it guarantees the delivery of network packets?

- A. TCP
- B. UDP
- C. SNMP
- D. ICMP

Answer: A

NEW QUESTION 8

What is the name of the attribute that specifies the name of the stanza in the transforms.conf file that defines the data transformation in the props.conf file?

- A. REGEX
- B. FORMAT
- C. DEST_KEY
- D. TRANSFORMS

Answer: D

NEW QUESTION 9

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 10

Which input type can be used to monitor Windows Registry Values for changes?

- A. WinRegMon
- B. WinRegistry
- C. WinRegValue
- D. WinRegChange

Answer: A

NEW QUESTION 10

What is the name of the dashboard that provides information on incoming data consumption and indexing rate for your Splunk Cloud Platform deployment?

- A. Indexing Performance
- B. Indexing Quality
- C. Indexing Status
- D. Indexing Overview

Answer: A

NEW QUESTION 12

Which attribute in outputs.conf can be used to specify the load balancing method for a group of forwarders?

- A. autoLB
- B. autoLBFrequency
- C. lb_method
- D. lb_poll

Answer: C

NEW QUESTION 13

Which feature allows a light forwarder to reduce the amount of data sent to the indexer by discarding some events or fields?

- A. Data cloning
- B. Data filtering
- C. Data sampling
- D. Data masking

Answer: C

NEW QUESTION 18

What is the name of the option that you need to check in Splunk Web to enable LDAP authentication for your Splunk Cloud Platform deployment?

- A. LDAP
- B. External
- C. LDAP/External
- D. External/LDAP

Answer: C

NEW QUESTION 19

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 24

Which input type can be used to monitor Windows Event Logs from a remote machine?

- A. WinEventLog
- B. WinEventLogCollections
- C. WinEventLogForwarder
- D. WinEventLogRemote

Answer: B

NEW QUESTION 26

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 31

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 32

Which type of forwarder is a legacy option that is not recommended for new deployments?

- A. Universal forwarder
- B. Heavy forwarder
- C. Light forwarder
- D. Deployment client

Answer: C

NEW QUESTION 37

Which command can be used to install a universal forwarder on a Linux system?

- A. splunk install forwarder
- B. splunk forwarder install
- C. splunk add forward-server
- D. splunk enable boot-start

Answer: A

NEW QUESTION 40

What is the name of the input processor that allows you to monitor files that Windows rotates automatically on machines that run Windows Vista or Windows Server 2008 and higher?

- A. monitor
- B. MonitorNoHandle
- C. upload
- D. UploadNoHandle

Answer: B

NEW QUESTION 44

Which type of forwarder has the lowest system resource usage and the highest data throughput?

- A. Universal forwarder
- B. Heavy forwarder
- C. Light forwarder
- D. Deployment client

Answer: A

NEW QUESTION 47

Which Splunk add-on simplifies the process of getting data into Splunk Cloud Platform from Windows Event Log channels?

- A. Splunk Add-on for Windows
- B. Splunk Add-on for Infrastructure
- C. Splunk Add-on for Active Directory
- D. Splunk Add-on for DNS

Answer: A

NEW QUESTION 48

.....

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](#)