

# Splunk

## Exam Questions SPLK-1005

Splunk Cloud Certified Admin



#### NEW QUESTION 1

What is the default value of the LINE\_BREAKER setting that splits the incoming stream of data into separate lines?

- A. Any sequence of newlines and carriage returns
- B. Any sequence of spaces and tabs
- C. Any sequence of punctuation marks
- D. Any sequence of alphanumeric characters

**Answer:** A

#### NEW QUESTION 2

What is the name of the attribute that specifies the sed script for data transformation in the props.conf file?

- A. SEDCMD
- B. FORMAT
- C. DEST\_KEY
- D. TRANSFORMS

**Answer:** A

#### NEW QUESTION 3

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 4

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 5

What is the name of the configuration file where you can define data transformations using regular expressions and other attributes?

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

**Answer:** D

#### NEW QUESTION 6

What is the name of the configuration file where you can specify the source type for a data input?

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

**Answer:** C

#### NEW QUESTION 7

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 8

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 9

Which feature of forwarders can prevent data loss in case of network failure or congestion?

- A. Data compression
- B. SSL security
- C. Configurable buffering
- D. Persistent queues

**Answer:** D

#### NEW QUESTION 10

What is the main advantage of managed Splunk Cloud over self-service Splunk Cloud in terms of scalability and reliability?

- A. Managed Splunk Cloud provides a single-instance environment that can scale up to 10TB/day and offers a 100% uptime SLA.
- B. Managed Splunk Cloud provides a clustered environment that can scale up to 10TB/day and offers a 100% uptime SLA.
- C. Managed Splunk Cloud provides a single-instance environment that can scale up to 5TB/day and offers a 99.9% uptime SLA.
- D. Managed Splunk Cloud provides a clustered environment that can scale up to 5TB/day and offers a 99.9% uptime SLA.

**Answer:** B

#### NEW QUESTION 10

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 15

What is the name of the Splunk Enterprise feature that provides a security data and event management (SIEM) solution that uses machine data to detect and respond to threats?

- A. Splunk Enterprise Security
- B. Splunk Enterprise Intelligence
- C. Splunk Enterprise Analytics
- D. Splunk Enterprise Monitoring

**Answer:** A

#### NEW QUESTION 20

Which configuration file needs to be edited to configure the universal forwarder to act as a deployment client?

- A. deploymentclient.conf
- B. server.conf
- C. outputs.conf
- D. inputs.conf

**Answer:** A

#### NEW QUESTION 21

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 23

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 24**

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 26**

Which setting in inputs.conf can be used to specify the interval at which the script runs for a scripted input?

- A. interval
- B. frequency
- C. schedule
- D. cron

**Answer:** A

**NEW QUESTION 27**

What is the name of the directory that contains all the Splunk indexes and other important data??

- A. /bin
- B. /var
- C. /etc
- D. /lib

**Answer:** B

**NEW QUESTION 29**

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 30**

Which type of metadata can be used to identify the origin of the data?

- A. Source
- B. Source type
- C. Host
- D. Index

**Answer:** C

**NEW QUESTION 35**

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 39**

What is the name of the tab in Splunk Web where you can set the indexes that a role can access?

- A. Inheritance
- B. Capabilities
- C. Indexes
- D. Restrictions

**Answer:** C

**NEW QUESTION 40**

Which type of forwarder can act as an intermediate forwarder to receive data from other forwarders and send it to the indexer?

- A. Universal forwarder
- B. Heavy forwarder
- C. Light forwarder
- D. Any type of forwarder

**Answer:** B

**NEW QUESTION 44**

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 47**

Which file processor can be used to index files that are locked by another process on Windows systems?

- A. Monitor
- B. MonitornoHandle
- C. Upload
- D. None of the above

**Answer:** B

**NEW QUESTION 52**

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 53**

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 56**

.....

## 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](#)**