

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

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

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 4

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 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

Which configuration file parameter can be used to modify line termination settings interactively, using the Set Source Type page in Splunk Web?

- A. LINE_BREAKER
- B. SHOULD_LINEMERGE
- C. BREAK_ONLY_BEFORE
- D. TRUNCATE

Answer: B

NEW QUESTION 7

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 8

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 9

Which command can be used to download and install the universal forwarder software on a Linux system?

- A. `wget -O splunkforwarder-<version>-Linux-x86_64.tgz 'https://www.splunk.com/bin/splunk/DownloadActivityServlet?architecture=x86_64&platform=linux&ve`
- B. `tar xvfz splunkforwarder-<version>-Linux-x86_64.tgz -C /opt`
- C. `/opt/splunkforwarder/bin/splunk start --accept-license`
- D. All of the above

Answer: D

NEW QUESTION 10

What are the three types of data that indexes contain in Splunk Cloud?

- A. Raw data, index data, and metadata
- B. Raw data, event data, and metadata
- C. Raw data, index data, and event data
- D. Raw data, index data, and metrics data

Answer: A

NEW QUESTION 10

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 12

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 17

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 22

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 26

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 28

What are the two options for Dynamic Data Storage in Splunk Cloud that allow you to move expired data from indexes to another storage location?

- A. Splunk Archive and Self Storage
- B. Splunk Backup and Self Storage
- C. Splunk Archive and Splunk Backup
- D. Self Storage and Splunk Restore

Answer: A

NEW QUESTION 33

What is the name of the Splunk Cloud feature that allows you to monitor and manage resource utilization by business units and users using a Splunk app?

- A. Splunk App for Chargeback
- B. Splunk App for Resource Management
- C. Splunk App for Usage Analytics
- D. Splunk App for Cost Optimization

Answer: A

NEW QUESTION 34

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 37

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 42

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 45

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 49

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 51

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 56

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 57

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 60

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 63

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 66

Which file processor can be used to index files that are not actively written to or updated?

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

Answer: C

NEW QUESTION 67

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 72

What is the name of the configuration file where you can set custom rules for event line breaking and line merging for a specific app?

- A. inputs.conf
- B. outputs.conf

- C. props.conf
- D. transforms.conf

Answer: C

NEW QUESTION 76

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 80

What is the name of the time standard that is the basis for time and time zones worldwide and does not change for Daylight Saving Time (DST)?

- A. GMT
- B. UTC
- C. PST
- D. BST

Answer: B

NEW QUESTION 85

What is the name of the configuration file that you need to edit to enable Data Preview for the search app?

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

Answer: A

NEW QUESTION 90

What is the name of the configuration file where you can invoke data transformations by associating them with a host, source, or source type?

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

Answer: B

NEW QUESTION 95

Which command can be used to install the Splunk universal forwarder credentials package on the universal forwarder machine?

- A. splunk install app <path_to_credentials_package>
- B. splunk add app <path_to_credentials_package>
- C. splunk install forwarder-credentials <path_to_credentials_package>
- D. splunk add forwarder-credentials <path_to_credentials_package>

Answer: A

NEW QUESTION 97

What is the name of the Splunk Cloud feature that allows you to perform self-service administrative tasks such as creating indexes, inputs, and roles?

- A. Admin Config Service
- B. Admin Console
- C. Admin Dashboard
- D. Admin Toolkit

Answer: A

NEW QUESTION 102

.....

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](#)