

SPLK-1005 Dumps

Splunk Cloud Certified Admin

<https://www.certleader.com/SPLK-1005-dumps.html>



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 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 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 5

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 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 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 8

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 9

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 10

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 10

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 11

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 15

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 18

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 21

Which command can be used to add a data input using the CLI?

- A. splunk add input
- B. splunk add monitor
- C. splunk add data
- D. splunk add source

Answer: B

NEW QUESTION 25

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 28

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 33

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 38

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 39

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 43

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 45

.....

Thank You for Trying Our Product

* 100% Pass or Money Back

All our products come with a 90-day Money Back Guarantee.

* One year free update

You can enjoy free update one year. 24x7 online support.

* Trusted by Millions

We currently serve more than 30,000,000 customers.

* Shop Securely

All transactions are protected by VeriSign!

100% Pass Your SPLK-1005 Exam with Our Prep Materials Via below:

<https://www.certleader.com/SPLK-1005-dumps.html>