

Exam Questions SPLK-1005

Splunk Cloud Certified Admin

<https://www.2passeasy.com/dumps/SPLK-1005/>



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

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 4

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 5

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 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 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 8

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 9

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

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 10

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 13

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

- A. Self-service Splunk Cloud costs less to get started and maintain and allows your organization total control in setup and security configurations.
- B. Self-service Splunk Cloud costs more to get started and maintain but allows your organization total control in setup and security configurations.
- C. Self-service Splunk Cloud costs less to get started and maintain but requires your organization to rely on Splunk for setup and security configurations.
- D. Self-service Splunk Cloud costs more to get started and maintain and requires your organization to rely on Splunk for setup and security configurations.

Answer: A

NEW QUESTION 15

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 17

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 20

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 21

.....

THANKS FOR TRYING THE DEMO OF OUR PRODUCT

Visit Our Site to Purchase the Full Set of Actual SPLK-1005 Exam Questions With Answers.

We Also Provide Practice Exam Software That Simulates Real Exam Environment And Has Many Self-Assessment Features. Order the SPLK-1005 Product From:

<https://www.2passeasy.com/dumps/SPLK-1005/>

Money Back Guarantee

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