

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

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 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

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 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 9

Which command can be used to run a 'splunk diag' on both the indexer and the forwarder?

- A. splunk diag -collect all -uri https://<username>:<password>@<host>:<port>
- B. splunk diag -collect all -auth <username>:<password>
- C. splunk diag -collect all -server <host>:<port>
- D. splunk diag -collect all -user <username> -password <password>

Answer: B

NEW QUESTION 10

Which type of forwarder is a full Splunk Enterprise instance that can run apps and add-ons?

- A. Universal forwarder
- B. Heavy forwarder
- C. Deployment server
- D. Search head

Answer: B

NEW QUESTION 10

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 11

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 12

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 17

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 20

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 25

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 29

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 32

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 35

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 36

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 39

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 44

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 46

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 49

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 52

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 57

What is the name of the component that acts as a data manager and sends data to Splunk Cloud Platform indexers?

- A. Heavy forwarder
- B. Universal forwarder
- C. Deployment server
- D. License master

Answer: A

NEW QUESTION 60

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 65

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 70

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 72

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 75

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 80

Which Windows-specific input type allows Splunk software to read special Windows log files such as the DNS debug server log?

- A. MonitorNoHandle
- B. Windows Event Log
- C. Windows Registry
- D. Windows Management Instrumentation (WMI)

Answer: A

NEW QUESTION 82

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 86

Which feature of forwarders can improve the network performance and reduce the bandwidth consumption?

- A. Data compression
- B. SSL security
- C. Data sampling
- D. Data filtering

Answer: A

NEW QUESTION 90

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 91

.....

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