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 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 3
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 4
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 5
Which feature allows a heavy forwarder to route data to different indexers based on criteria such as source, sourcetype, or host?

A. Data cloning
B. Data filtering
C. Data sampling
D. Data masking

Answer: A

NEW QUESTION 6
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 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
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 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 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 13
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 17
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 20
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 24
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 26
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 27
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 32
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 36
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 39
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 40
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 41
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 43
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 44
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 46
......

Thank You for Trying Our Product

We offer two products:

1st - We have Practice Tests Software with Actual Exam Questions

2nd - Questons 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