Splunk

Exam Questions SPLK-1005

Splunk Cloud Certified Admin

NEW QUESTION 1
Which configuration file determines how a universal forwarder forwards data to the indexer?

A. inputs.conf
B. outputs.conf
C. props.conf
D. transforms.conf

Answer: B

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 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 4
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 5
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 6
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 7
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 8
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 9
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 10
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 10
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 13
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 18
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 22
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 can perform data parsing and enrichment before sending it to the indexer?

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

Answer: B

NEW QUESTION 26
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 29
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 32
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 36
Which option can be used to specify the host value of the data when creating a file or directory monitor input?

A. Set Host
B. Select Host
C. Choose Host
D. Define Host

Answer: A

NEW QUESTION 39
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 42
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 43
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 45
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 49
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 51
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 52
......

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