Splunk

Exam Questions SPLK-1005

Splunk Cloud Certified Admin

NEW QUESTION 1
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 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
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 5
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 6
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 7
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 8
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 9
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 10
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 10
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 12
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 14
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 15
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 20
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 22
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 23
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 26
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 29
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 34
......

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