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
Which network protocol is recommended for sending data to Splunk because it guarantees the delivery of network packets?

A. TCP
B. UDP
C. SNMP
D. ICMP

Answer: A

NEW QUESTION 3
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 4
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 5
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 6
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 7
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 8
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 9
What is the name of the Splunk Cloud feature that allows you to get data from APIs and other remote data interfaces through scripted inputs?

A. Splunk Cloud Data Connectors
B. Splunk Cloud Data Integrations
C. Splunk Cloud Data Collectors
D. Splunk Cloud Data Sources

Answer: C

NEW QUESTION 10
What is the regular expression format that represents any sequence of newlines and carriage returns, which is the default value of the LINE_BREAKER setting?

A. ([\r\n]+)
B. ([\s]+)
C. ([\w]+)
D. ([\p]+)

Answer: A

NEW QUESTION 10
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 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 18
Which type of forwarder can act as an intermediate forwarder to receive data from other forwarders and send it to the indexer?

A. Universal forwarder
B. Heavy forwarder
C. Light forwarder
D. Any type of forwarder

Answer: B

NEW QUESTION 20
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 24
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 27
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 32
.....

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