Splunk

Exam Questions SPLK-1005

Splunk Cloud Certified Admin

NEW QUESTION 1
What is the name of the attribute that specifies the sed script for data transformation in the props.conf file?

A. SEDCMD
B. FORMAT
C. DEST_KEY
D. TRANSFORMS

Answer: A

NEW QUESTION 2
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 3
Which setting in inputs.conf can be used to specify the SSL certificate for a TCP or UDP input?

A. sslCertPath
B. sslRootCAPath
C. sslPassword
D. All of the above

Answer: D

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
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
Which setting in inputs.conf can be used to specify the command to run the script for a scripted input?

A. script
B. command
C. exec
D. run

Answer: C

NEW QUESTION 7
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 8
What are the three types of data that indexes contain in Splunk Cloud?

A. Raw data, index data, and metadata
B. Raw data, event data, and metadata
C. Raw data, index data, and event data
D. Raw data, index data, and metrics data

Answer: A

NEW QUESTION 9
What is the name of the attribute that specifies the name of the stanza in the transforms.conf file that defines the data transformation in the props.conf file?

A. REGEX
B. FORMAT
C. DEST_KEY
D. TRANSFORMS

Answer: D

NEW QUESTION 10
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 10
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 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 16
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 19
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 23
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 26
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 29
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 33
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 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 38
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 43
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 46
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 51
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 53
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 58
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 59
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 61
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 64
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 69
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 70
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 71
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 75
Which setting in inputs.conf can be used to specify the SSL certificate for a TCP or UDP input?

A. sslCertPath
B. sslRootCAPath
C. sslPassword
D. All of the above

Answer: D

NEW QUESTION 80
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 85
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 89
......