Splunk

Exam SPLK-1005

Splunk Cloud Certified Admin

Version: 3.0

[Total Questions: 73]

Question No : 1

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

Question No : 2

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

Question No : 3

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

Question No : 4

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

Question No : 5

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

Question No : 6

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

Question No : 7

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

Question No : 8

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

Question No : 9

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

Question No : 10

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

Question No : 11

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

Question No : 12

Which feature of forwarders can protect the data from unauthorized access or tampering?

A. Data compression
B. SSL security
C. Data masking
D. Data encryption

Answer: B

Question No : 13

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

Question No : 14

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

Question No : 15

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

Question No : 16

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

Question No : 17

What are the four default roles that Splunk Cloud Platform comes with?

A. admin, power, user, can_delete
B. admin, power, user, sc_admin
C. admin, power, user, guest
D. admin, power, user, can_write

Answer: B

Question No : 18

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

Question No : 19

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

Question No : 20

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

Question No : 21

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

Question No : 22

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

Question No : 23

What is the name of the configuration file that governs data inputs such as forwarders and file system monitoring?

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

Answer: A

Question No : 24

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

Question No : 25

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

Question No : 26

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

Question No : 27

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

Question No : 28

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

Question No : 29