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 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 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

NEW QUESTION 4
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 5
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 6
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 7
Which input type can be used to monitor Windows Registry Values for changes?

A. WinRegMon
B. WinRegistry
C. WinRegValue
D. WinRegChange

Answer: A

NEW QUESTION 8
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 9
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 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 10
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 12
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 13
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 17
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 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 23
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 27
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 29
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 34
What is the name of the tab in Splunk Web where you can set the indexes that a role can access?

A. Inheritance
B. Capabilities
C. Indexes
D. Restrictions

Answer: C

NEW QUESTION 38
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 40
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

NEW QUESTION 42
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 46
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 51
What is the name of the time standard that is the basis for time and time zones worldwide and does not change for Daylight Saving Time (DST)?

A. GMT
B. UTC
C. PST
D. BST

Answer: B

NEW QUESTION 56
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 57
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 62
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 65
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 68
......