Splunk

Exam Questions SPLK-1005

Splunk Cloud Certified Admin

NEW QUESTION 1
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

NEW QUESTION 2
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 3
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 4
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 5
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 6
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 7
Which command can be used to run a ‘splunk diag’ on both the indexer and the forwarder?

A. splunk diag -collect all -uri https://<username>:<password>@<host>:<port>
B. splunk diag -collect all -auth <username>:<password>
C. splunk diag -collect all -server <host>:<port>
D. splunk diag -collect all -user <username> -password <password>

Answer: B

NEW QUESTION 8
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 9
Which command can be used to download and install the universal forwarder software on a Linux system?

A. wget -O splunkforwarder-<version>-Linux-x86_64.tgz ‘https://www.splunk.com/bin/splunk/DownloadActivityServlet?architecture=x86_64&platform=linux&ve
B. tar xvzf splunkforwarder-<version>-Linux-x86_64.tgz -C /opt
C. /opt/splunkforwarder/bin/splunk start --accept-license
D. All of the above

Answer: D

NEW QUESTION 10
What is the name of the configuration file where you can specify the source type for a data input?

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

Answer: C

NEW QUESTION 10
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 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

NEW QUESTION 14
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

NEW QUESTION 15
What is the name of the Splunk Enterprise feature that provides a security data and event management (SIEM) solution that uses machine data to detect and respond to threats?

A. Splunk Enterprise Security
B. Splunk Enterprise Intelligence
C. Splunk Enterprise Analytics
D. Splunk Enterprise Monitoring

Answer: A

NEW QUESTION 17
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 18
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 23
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 25
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 28
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 32
Which setting in inputs.conf can be used to specify the interval at which the script runs for a scripted input?

A. interval
B. frequency
C. schedule
D. cron

Answer: A

NEW QUESTION 34
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 42

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 46
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 49
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 51
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 52
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 53
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 56
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 59
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 63
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 64
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 65
Which Splunk add-on simplifies the process of getting data into Splunk Cloud Platform from Windows Event Log channels?

A. Splunk Add-on for Windows
B. Splunk Add-on for Infrastructure
C. Splunk Add-on for Active Directory
D. Splunk Add-on for DNS

Answer: A

NEW QUESTION 69
What is the name of the configuration file that you need to edit to enable Data Preview for the search app?

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

Answer: A

NEW QUESTION 74
......