Splunk

Exam Questions SPLK-1005

Splunk Cloud Certified Admin

NEW QUESTION 1
What is the default value of the LINE_BREAKER setting that splits the incoming stream of data into separate lines?

A. Any sequence of newlines and carriage returns
B. Any sequence of spaces and tabs
C. Any sequence of punctuation marks
D. Any sequence of alphanumeric characters

Answer: A

NEW QUESTION 2
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 3
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 4
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 5
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 6
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 7
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

NEW QUESTION 8
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 9
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 10
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 10
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 15
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 20
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 23
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 25
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 28
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 32
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 37
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 42
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 44
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 47
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 49
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 50

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 54
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 55
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 56
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 60
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 63
What is the name of the first step that you need to perform to configure the LDAP authentication scheme with Splunk Web?

A. Create an LDAP strategy
B. Map LDAP groups to Splunk roles
C. Configure LDAP settings
D. Test LDAP connection

Answer: A

NEW QUESTION 65
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 66
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 68
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 73
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 78
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 83
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 86
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 87
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 89
.....

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