SPLK-1003Q&As

Splunk Enterprise Certified Admin

Pass Splunk SPLK-1003 Exam with 100% Guarantee

Free Download Real Questions & Answers **PDF** and **VCE** file from:

https://www.pass2lead.com/splk-1003.html

100% Passing Guarantee
100% Money Back Assurance

Following Questions and Answers are all new published by Splunk Official Exam Center

- **Instant Download** After Purchase
- **100% Money Back** Guarantee
- **365 Days** Free Update
- **800,000+** Satisfied Customers

QUESTION 1

What is the default value of LINE_BREAKER?

A. \r\n

B. ([\r\n]+)

C. \r+\n+

D. (\r\n+)

Correct Answer: B

Line breaking, which uses the LINE_BREAKER setting to split the incoming stream of data into separate lines. By default, the LINE_BREAKER value is any sequence of newlines and carriage returns. In regular expression format, this is represented as the following string: ([\r\n]+). You don\\'t normally need to adjust this setting, but in cases where it\\'s necessary, you must configure it in the props.conf configuration file on the forwarder that sends the data to Splunk Cloud Platform or a Splunk Enterprise indexer. The LINE_BREAKER setting expects a value in regular expression format.

Reference: https://docs.splunk.com/Documentation/SplunkCloud/8.2.2105/Data/Configureeventlinebreaking

QUESTION 2

What are the required stanza attributes when configuring the transforms. conf to manipulate or remove events?

A. REGEX, DEST. FORMAT

B. REGEX. SRC_KEY, FORMAT

C. REGEX, DEST_KEY, FORMAT

D. REGEX, DEST_KEY FORMATTING

Correct Answer: C

REGEX =

*

Enter a regular expression to operate on your data. FORMAT =

*

NOTE: This option is valid for both index-time and search-time field extraction. Index-time field extraction configuration require the FORMAT settings. The FORMAT settings is optional for search-time field extraction configurations.

*

This setting specifies the format of the event, including any field names or values you want to add. DEST_KEY =

*

NOTE: This setting is only valid for index-time field extractions.

*

Specifies where SPLUNK software stores the expanded FORMAT results in accordance with the REGEX match.

QUESTION 3

In which phase of the index time process does the license metering occur?

A. input phase

B. Parsing phase

C. Indexing phase

D. Licensing phase

Correct Answer: C

"When ingesting event data, the measured data volume is based on the new raw data that is placed into the indexing pipeline. Because the data is measured at the indexing pipeline, data that is filetered and dropped prior to indexing does not count against the license volume qota."
https://docs.splunk.com/Documentation/Splunk/8.0.6/Admin/HowSplunklicensingworks

QUESTION 4

In which Splunk configuration is the SEDCMD used?

A. props, conf

B. inputs.conf

C. indexes.conf

D. transforms.conf

Correct Answer: A

https://docs.splunk.com/Documentation/Splunk/8.0.5/Forwarding/Forwarddatatothird- partysystemsd

QUESTION 5

Which of the following statements describes how distributed search works?

A. Forwarders pull data from the search peers.

B. Search heads store a portion of the searchable data.

C. The search head dispatches searches to the search peers.

D. Search results are replicated within the indexer cluster.

Correct Answer: C

https://docs.splunk.com/Documentation/Splunk/8.2.2/DistSearch/Configuredistributedsearch

"To activate distributed search, you add search peers, or indexers, to a Splunk Enterprise instance that you desingate as a search head. You do this by specifying each search peer manually."

QUESTION 6

When Splunk is integrated with LDAP, which attribute can be changed in the Splunk UI for an LDAP user?

A. Default app

B. LDAP group

C. Password

D. Username

Correct Answer: B

Reference: https://docs.splunk.com/Documentation/Splunk/8.2.3/Security/ConfigureLDAPwithSplunkWeb

QUESTION 7

An organization wants to collect Windows performance data from a set of clients, however, installing Splunk software on these clients is not allowed. What option is available to collect this data in Splunk Enterprise?

A. Use Local Windows host monitoring.

B. Use Windows Remote Inputs with WMI.

C. Use Local Windows network monitoring.

D. Use an index with an Index Data Type of Metrics.

Correct Answer: B

https://docs.splunk.com/Documentation/Splunk/8.1.0/Data/ConsiderationsfordecidinghowtomonitorWindowsdata

"The Splunk platform collects remote Windows data for indexing in one of two ways: From Splunk forwarders, Using Windows Management Instrumentation (WMI). For Splunk Cloud deployments, you must use the Splunk Universal Forwarder on a Windows machines to montior remote Windows data."

QUESTION 8

Which of the following configuration files are used with a universal forwarder? (Choose all that apply.)

A. inputs.conf

B. monitor.conf

C. outputs.conf

D. forwarder.conf

Correct Answer: AC

Reference:

https://docs.splunk.com/Documentation/Forwarder/8.0.5/Forwarder/ Configuretheuniversalforwarder

QUESTION 9

Which of the following are available input methods when adding a file input in Splunk Web? (Choose all that apply.)

A. Index once.

B. Monitor interval.

C. On-demand monitor.

D. Continuously monitor.

Correct Answer: AD

https://docs.splunk.com/Documentation/Splunk/8.2.2/Data/Howdoyouwanttoadddata

The fastest way to add data to your Splunk Cloud instance or Splunk Enterprise deployment is to use Splunk Web. After you access the Add Data page, choose one of three options for getting data into your Splunk platform deployment with Splunk Web: (1) Upload, (2) Monitor, (3) Forward The Upload option lets you upload a file or archive of files for indexing. When you choose Upload option, Splunk Web opens the upload process page. Monitor. For Splunk Enterprise installations, the Monitor option lets you monitor one or more files, directories, network streams, scripts, Event Logs (on Windows hosts only), performance metrics, or any other type of machine data that the Splunk Enterprise instance has access to.

QUESTION 10

When does a warm bucket roll over to a cold bucket?

A. When Splunk is restarted.

B. When the maximum warm bucket age has been reached.

C. When the maximum warm bucket size has been reached.

D. When the maximum number of warm buckets is reached.

Correct Answer: D

Once further conditions are met (for example, the index reaches some maximum number of warm buckets), the indexer begins to roll the warm buckets to cold, based on their age. It always selects the oldest warm bucket to roll to cold. Buckets continue to roll to cold as they age in this manner. Cold buckets reside in a different location from hot and warm

buckets. You can configure the location so that cold buckets reside on cheaper storage.

Reference: https://community.splunk.com/t5/Deployment-Architecture/Rolling-Hot-Data-to-to-Cold-quicker/tdp/166653

QUESTION 11

User role inheritance allows what to be inherited from the parent role? (select all that apply)

A. Parents

B. Capabilities

C. Index access

D. Search history

Correct Answer: BC

https://docs.splunk.com/Documentation/Splunk/latest/Security/Aboutusersandroles#Role_i nheritance
https://docs.splunk.com/Documentation/Splunk/7.3.1/Security/Aboutusersandroles#How_users_inherit_capabilities

QUESTION 12

What is the default character encoding used by Splunk during the input phase?

A. UTF-8

B. UTF-16

C. EBCDIC

D. ISO 8859

Correct Answer: A

https://docs.splunk.com/Documentation/Splunk/7.3.1/Data/Configurecharactersetencoding

"Configure character set encoding. Splunk software attempts to apply UTF-8 encoding to your scources by default. If a source foesn\\'t use UTF-8 encoding or is a non-ASCII file, Splunk software tries to convert data from the source to UTF-8 encoding unless you specify a character set to use by setting the CHARSET key in the props.conf file."

QUESTION 13

Which of the following statements describe deployment management? (select all that apply)

A. Requires an Enterprise license

B. Is responsible for sending apps to forwarders.

C. Once used, is the only way to manage forwarders

D. Can automatically restart the host OS running the forwarder.

Correct Answer: AB

https://docs.splunk.com/Documentation/Splunk/8.2.2/Admin/Distdeploylicenses#:~:text=License%20requirements,do%20not%20index%20external%20data.

"All Splunk Enterprise instances functioning as management components needs access to an Enterprise license. Management components include the deployment server, the indexer cluster manager node, the search head cluster deployer, and the monitoring console."

https://docs.splunk.com/Documentation/Splunk/8.2.2/Updating/Aboutdeploymentserver

"The deployment server is the tool for distributing configurations, apps, and content updates to groups of Splunk Enterprise instances."

QUESTION 14

Where should apps be located on the deployment server that the clients pull from?

A. $SFLUNK_KOME/etc/apps

B. $SPLUNK_HCME/etc/sear:ch

C. $SPLUNK_HCME/etc/master-apps

D. $SPLUNK HCME/etc/deployment-apps

Correct Answer: D

QUESTION 15

Which of the following is accurate regarding the input phase?

A. Breaks data into events with timestamps.

B. Applies event-level transformations.

C. Fine-tunes metadata.

D. Performs character encoding.

Correct Answer: D

"The data pipeline segments in depth. INPUT - In the input segment, Splunk software consumes data. It acquires the raw data stream from its source, breaks it into 64K blocks, and annotates each block with some metadata keys. The keys can also include values that are used internally, such as the character encoding of the data stream, and values that control later processing of the data, such as the index into which the events should be stored. PARSING Annotating individual events with metadata copied from the source-wide keys. Transforming event data and metadata according to regex transform rules."

SPLK-1003 VCE Dumps SPLK-1003 Study Guide SPLK-1003 Braindumps