Splunk SPLK-1005 Practice Questions

Shared by Price on 18-08-2026

For More Free Questions and Preparation Resources

Check the Links on Last Page

Question 1

Question Type: MultipleChoice

A monitor has been created in inputs. con: for a directory that contains a mix of file types.

How would a Cloud Admin fine-tune assigned sourcetypes for different files in the directory during the input phase?

Options:

A- On the Indexer parsing the data, leave sourcetype as automatic for the directory monitor. Then create a props.conf that assigns a specific sourcetype by source stanza.
B- On the forwarder collecting the data, leave sourcetype as automatic for the directory monitor. Then create a props. conf that assigns a specific sourcetype by source stanza.
C- On the Indexer parsing the data, set multiple sourcetype_source attributes for the directory monitor collecting the files. Then create a props, com that filters out unwanted files.
D- On the forwarder collecting the data, set multiple 3ourcotype_sourc attributes for the directory monitor collecting the files. Then create a props. conf that filters out unwanted files.

Answer:

B

Explanation:

When dealing with a directory containing a mix of file types, it's essential to fine-tune the sourcetypes for different files to ensure accurate data parsing and indexing.

B . On the forwarder collecting the data, leave sourcetype as automatic for the directory monitor. Then create a props.conf that assigns a specific sourcetype by source stanza: This is the correct answer. In this approach, the Universal Forwarder is set up with a directory monitor where the sourcetype is initially left as automatic. Then, a props.conf file is configured to specify different sourcetypes based on the source (filename or path). This ensures that as the data is collected, it is appropriately categorized by sourcetype according to the file type.

Splunk Documentation Reference:

Configuring Inputs and Sourcetypes

Fine-tuning sourcetypes

Question 2

Question Type: MultipleChoice

Configuration folders named default contain configuration files/settings specified in the Splunk product or default settings specified in apps. Which of the following is recommended to override these settings?

Options:

A- It does not matter whether setting overrides are placed in default or local folders. Both are equally acceptable since Splunk will merge all the files together into one runtime model after each restart.
B- Any settings to be overridden should be modified in-place wherever the setting was found originally. For example, if overriding a setting originally found in system/default, it should be overridden there to ensure that the desired value is used by Splunk.
C- Overrides should be placed in a folder named local, ideally within a custom Splunk app. This ensures the overrides are preserved upon product or app upgrade and will also be easier to maintain/support.
D- Try to store all configuration overrides in system/local folder to keep all configurations in one place. This ensures the modification has the highest precedence over all other configuration entries.

Answer:

C

Explanation:

Placing configuration overrides in the local folder within a custom app allows for easy maintenance and ensures that these overrides are preserved during upgrades, as files in default are overwritten. [Reference: Splunk Docs on configuration file precedence]

Question 3

Question Type: MultipleChoice

Which of the following is a valid monitor stanza for inputs.conf?

Options:

A- [monitor:///var/log/*.log] index = linux sourcetype = access_combined host = 489307057
B- [monitor:\\\var\log\httpd-[0-9].log] index = linux sourcetype = access_combined host = 489307057
C- [monitor:///var/log/httpd-[0-9].log] index = linux sourcetype = access_combined host = 489307057
D- [monitor:\\\var\log*.log] index = linux sourcetype = access_combined host = 489307057

Answer:

C

Explanation:

[monitor:///var/log/httpd-[0-9].log] is a valid path and syntax for inputs.conf to monitor files ending in .log under /var/log, with other correct index, sourcetype, and host settings specified. [Reference: Splunk Docs on monitor stanzas]

Question 4

Question Type: MultipleChoice

Which of the following is a valid method to test if a forwarder can successfully send data to Splunk Cloud?

Options:

A- Search the _audit index to confirm whether the forwarder ID was registered.
B- Use oneshot from the CLI on the forwarders, then check to see if those logs show up in the Splunk Cloud environment.
C- On Splunk Cloud UI, click Add Data and upload a test file, then search to see if the logs show up.
D- Ping the inputssl.example.splunkcloud.com to see if it returns the ping.

Answer:

B

Explanation:

Using the oneshot command allows a direct check for data reception in the cloud environment. Logs can be verified in the cloud after the forwarder sends them. [Reference: Splunk Docs on testing forwarder data inputs]

Question 5

Question Type: MultipleChoice

A customer wants to mask unstructured data before sending it to Splunk Cloud. Where should SEBCMD be configured for this?

Options:

A- props. conf on a Splunk Cloud search head,
B- props.conf on a Heavy Forwarder.
C- transforms, cent on a Splunk Cloud indexer.
D- props. conf- on a Universal Forwarder.

Answer:

B

Explanation:

To mask unstructured data before sending it to Splunk Cloud, the SEDCMD should be configured in the props.conf file on a Heavy Forwarder. The Heavy Forwarder is responsible for data parsing and transformation before forwarding the data to Splunk Cloud. This ensures that sensitive data is masked before it reaches the indexing stage.

Splunk Documentation Reference: Using SEDCMD to Mask Data

Question 6

Question Type: MultipleChoice

Which monitor statement will retrieve only files that start with "access" in the directory /opt/log/ww2/?

```
ll /opt/log/www2/
-rw-r--r-- 1 root root 32841910 May  7 22:32 access.log
-rw-r--r-- 1 root root   844129 May  7 22:37 secure.log
```

Options:

A- [monitor:///opt/lug/.../access]
B- [monitor:///opt/log/www2/access*]
C- [monitor:///opt/log/www2/]
D- [monitor:///opt/log/.../]

Answer:

B

Explanation:

The correct monitor statement to retrieve only files that start with 'access' in the directory /opt/log/www2/ is [monitor:///opt/log/www2/access*]. This configuration specifically targets files that begin with the name 'access' and will match any such files within that directory, such as 'access.log'.

Splunk Documentation Reference: Monitor files and directories

Question 7

Question Type: MultipleChoice

What does the followTail attribute do in inputs.conf?

Options:

A- Pauses a file monitor if the queue is full.
B- Only creates a tail checkpoint of the monitored file.
C- Ingests a file starting with new content and then reading older events.
D- Prevents pre-existing content in a file from being ingested.

Answer:

D

Explanation:

The followTail attribute in inputs.conf controls how Splunk processes existing content in a monitored file.

D . Prevents pre-existing content in a file from being ingested: This is the correct answer. When followTail = true is set, Splunk will ignore any pre-existing content in a file and only start monitoring from the end of the file, capturing new data as it is added. This is useful when you want to start monitoring a log file but do not want to index the historical data that might be present in the file.

A . Pauses a file monitor if the queue is full: Incorrect, this is not related to the followTail attribute.

B . Only creates a tail checkpoint of the monitored file: Incorrect, while a tailing checkpoint is created for state tracking, followTail specifically refers to skipping the existing content.

C . Ingests a file starting with new content and then reading older events: Incorrect, followTail does not read older events; it skips them.

Splunk Documentation Reference:

followTail Attribute Documentation

Monitoring Files

These answers align with Splunk's best practices and available documentation on managing and configuring Splunk environments.

Question 8

Question Type: MultipleChoice

In case of a Change Request, which of the following should submit a support case for Splunk Support?

Options:

A- The party requesting the change.
B- Certified Splunk Cloud administrator.
C- Splunk infrastructure owner.
D- Any person with the appropriate entitlement

Answer:

D

Explanation:

In Splunk Cloud, when there is a need for a change request that might involve modifying settings, upgrading, or other actions requiring Splunk Support, the process typically requires submitting a support case.

D . Any person with the appropriate entitlement: This is the correct answer. Any individual who has the necessary permissions or entitlements within the Splunk environment can submit a support case. This includes administrators or users who have been granted the ability to engage with Splunk Support. The request does not necessarily have to come from a Certified Splunk Cloud Administrator or the infrastructure owner; rather, it can be submitted by anyone with the correct level of access.

Splunk Documentation Reference:

Submitting a Splunk Support Case

Managing User Roles and Entitlements

Question 9

Question Type: MultipleChoice

The following Apache access log is being ingested into Splunk via a monitor input:

```
192.2.14.109 my.webserver.example - - 443 [09/Sep/2020:06:35:25 -0400] "GET / HTTP/1.1" "" 200 409 "-" "Mozilla/5.0
(Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/60.0.3112.113 Safari/537.36" 502 3110 1705
```

How does Splunk determine the time zone for this event?

Options:

A- The value of the TZ attribute in props. cont for the a :ces3_ccwbined sourcetype.
B- The value of the TZ attribute in props, conf for the my.webserver.example host.
C- The time zone of the Heavy/Intermediate Forwarder with the monitor input.
D- The time zone indicator in the raw event data.

Answer:

D

Explanation:

In Splunk, when ingesting logs such as an Apache access log, the time zone for each event is typically determined by the time zone indicator present in the raw event data itself. In the log snippet you provided, the time zone is indicated by -0400, which specifies that the event's timestamp is 4 hours behind UTC (Coordinated Universal Time).

Splunk uses this information directly from the event to properly parse the timestamp and apply the correct time zone. This ensures that the event's time is accurately reflected regardless of the time zone in which the Splunk instance or forwarder is located.

Splunk Cloud Reference: For further details, you can review Splunk documentation on timestamp recognition and time zone handling, especially in relation to log files and data ingestion configurations.

Source:

Splunk Docs: How Splunk software handles timestamps

Splunk Docs: Configure event timestamp recognition