Splunk

SPLK-1005 Exam

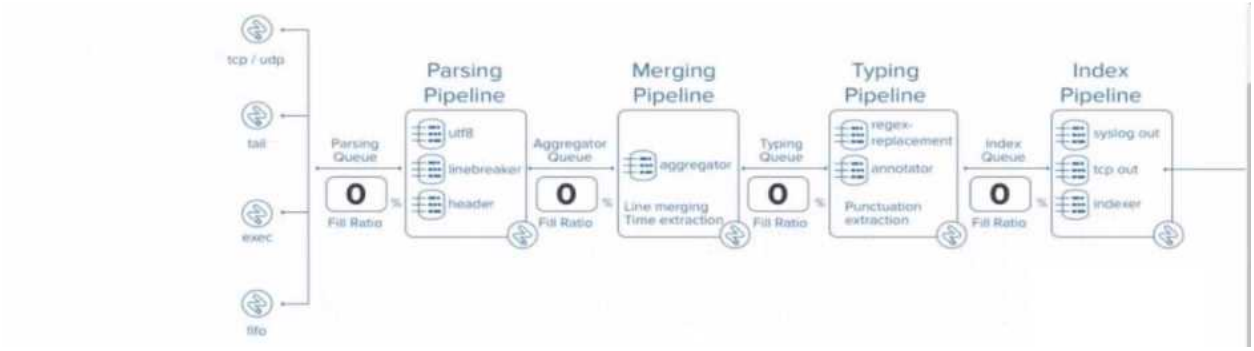
Splunk Cloud Certified Admin

Questions & Answers
Demo

Version: 4.0

Question: 1

At what point in the indexing pipeline set is SEDCMD applied to data?



A. In the aggregator queue
B. In the parsing queue
C. In the exec pipeline
D. In the typing pipeline

Answer: D

Explanation:

In Splunk, SEDCMD (Stream Editing Commands) is applied during the Typing Pipeline of the data indexing process. The Typing Pipeline is responsible for various tasks, such as applying regular expressions for field extractions, replacements, and data transformation operations that occur after the initial parsing and aggregation steps.
Here's how the indexing process works in more detail:
Parsing Pipeline: In this stage, Splunk breaks incoming data into events, identifies timestamps, and assigns metadata.
Merging Pipeline: This stage is responsible for merging events and handling time-based operations.
Typing Pipeline: The Typing Pipeline is where SEDCMD operations occur. It applies regular expressions and replacements, which is essential for modifying raw data before indexing. This pipeline is also responsible for field extraction and other similar operations.
Index Pipeline: Finally, the processed data is indexed and stored, where it becomes available for searching.
Splunk Cloud Reference: To verify this information, you can refer to the official Splunk documentation on the data pipeline and indexing process, specifically focusing on the stages of the indexing pipeline and the roles they play. Splunk Docs often discuss the exact sequence of operations within the pipeline, highlighting when and where commands like SEDCMD are applied during data processing.
Source:
Splunk Docs: Managing Indexers and Clusters of Indexers

Splunk Answers: Community discussions and expert responses frequently clarify where specific operations occur within the pipeline.

Question: 2

When monitoring directories that contain mixed file types, which setting should be omitted from inputs, conf and instead be overridden in propo.conf?

A. sourcetype
B. host
C. source
D. index

Answer: A

Explanation:

When monitoring directories containing mixed file types, the sourcetype should typically be overridden in props.conf rather than defined in inputs.conf. This is because sourcetype is meant to classify the type of data being ingested, and when dealing with mixed file types, setting a single sourcetype in inputs.conf would not be effective for accurate data classification. Instead, you can use props.conf to define rules that apply different sourcetypes based on the file path, file name patterns, or other criteria. This allows for more granular and accurate assignment of sourcetypes, ensuring the data is properly parsed and indexed according to its type.
Splunk Cloud Reference: For further clarification, refer to Splunk's official documentation on configuring inputs and props, especially the sections discussing monitoring directories and configuring sourcetypes.
Source:
Splunk Docs: Monitor files and directories
Splunk Docs: Configure event line breaking and input settings with props.conf

Question: 3

How are HTTP Event Collector (HEC) tokens configured in a managed Splunk Cloud environment?

A. Any token will be accepted by HEC, the data may just end up in the wrong index.
B. A token is generated when configuring a HEC input, which should be provided to the application developers.
C. Obtain a token from the organization's application developers and apply it in Settings > Data Inputs > HTTP Event Collector > New Token.
D. Open a support case for each new data input and a token will be provided.

Answer: B

Explanation:

In a managed Splunk Cloud environment, HTTP Event Collector (HEC) tokens are configured by an administrator through the Splunk Web interface. When setting up a new HEC input, a unique token is automatically generated. This token is then provided to application developers, who will use it to

authenticate and send data to Splunk via the HEC endpoint.
This token ensures that the data is correctly ingested and associated with the appropriate inputs and indexes. Unlike the other options, which either involve external tokens or support cases, option B reflects the standard procedure for configuring HEC tokens in Splunk Cloud, where control over tokens remains within the Splunk environment itself.
Splunk Cloud Reference: Splunk's documentation on HEC inputs provides detailed steps on creating and managing tokens within Splunk Cloud. This includes the process of generating tokens, configuring data inputs, and distributing these tokens to application developers.
Source:
Splunk Docs: HTTP Event Collector in Splunk Cloud Platform
Splunk Docs: Create and manage HEC tokens

Question: 4

Which of the following statements regarding apps in Splunk Cloud is true?

A. Self-service install of premium apps is possible.
B. Only Cloud certified and vetted apps are supported.
C. Any app that can be deployed in an on-prem Splunk Enterprise environment is also supported on Splunk Cloud.
D. Self-service install is available for all apps on Splunkbase.

Answer: B

Explanation:

In Splunk Cloud, only apps that have been certified and vetted by Splunk are supported. This is because Splunk Cloud is a managed service, and Splunk ensures that all apps meet specific security, performance, and compatibility requirements before they can be installed. This certification process guarantees that the apps won't negatively impact the overall environment, ensuring a stable and secure cloud service.
Self-service installation is available, but it is limited to apps that are certified for Splunk Cloud. Non-certified apps cannot be installed directly; they require a review and approval process by Splunk support.
Splunk Cloud Reference: Refer to Splunk's documentation on app installation and the list of Cloud-vetted apps available on Splunkbase to understand which apps can be installed in Splunk Cloud.
Source:
Splunk Docs: About apps in Splunk Cloud
Splunkbase: Splunk Cloud Apps

Question: 5

When using Splunk Universal Forwarders, which of the following is true?

A. No more than six Universal Forwarders may connect directly to Splunk Cloud.

B. Any number of Universal Forwarders may connect directly to Splunk Cloud.

C. Universal Forwarders must send data to an Intermediate Forwarder.

D. There must be one Intermediate Forwarder for every three Universal Forwarders.

Answer: B

Explanation:

Universal Forwarders can connect directly to Splunk Cloud, and there is no limit on the number of Universal Forwarders that may connect directly to it. This capability allows organizations to scale their data ingestion easily by deploying as many Universal Forwarders as needed without the requirement for intermediate forwarders unless additional data processing, filtering, or load balancing is required.
Splunk Documentation Reference: Forwarding Data to Splunk Cloud