DUMPSBOSS.

Splunk Core Certified User

Splunk SPLK-1001

Version Demo

Total Demo Questions: 29

Total Premium Questions: 294

Buy Premium PDF

https://dumpsboss.co

support@dumpsboss.co

support@dumpsboss.co
dumpsboss.co

Topic Break Down

Topic	No. of Questions
Topic 1, Splunk Basics	89
Topic 2, Basic Searching	34
Topic 3, Using Fields in Searches	47
Topic 4, Search Language Fundamentals	32
Topic 5, Basic Transforming Commands	45
Topic 6, Creating Reports and Dashboards	19
Topic 7, Creating and Using Lookups	17
Topic 8, Creating Scheduled Reports and Alerts	10
Topic 9, Mix Questions	1
Total	294

QUESTION NO: 1

Machine data can be in structured and unstructured format.

A. False

B. True

ANSWER: B

Explanation:

Machine data can be structured, unstructured, or semi-structured, so “True” is correct. Structured machine data follows a consistent and predefined schema, such as records from a relational database or fixed-format application output. Unstructured machine data does not conform to a fixed schema and may include free-form text, messages, or other variable content. Much of the operational data sent to Splunk is also semi-structured, such as log events containing key-value pairs or JSON fields. Splunk is designed to ingest and search across these different data forms. During ingestion, Splunk separates incoming data into events and can extract or recognize fields from formats such as JSON, CSV, XML, and key-value data. This flexibility lets users investigate operational activity even when the underlying sources use different formats and levels of organization. Splunk’s documentation describes machine data broadly as data generated by applications, servers, devices, and other technology components, and explains how Splunk processes that data for search and analysis. See the Splunk overview of machine data and the Splunk documentation on data Splunk can index.

QUESTION NO: 2

The stats command will create a _____ by default.

A. Table

B. Report

C. Pie chart

ANSWER: A

Explanation:

Table is correct because `stats` is a transforming SPL command: it calculates aggregate values over the search results and returns those values as a tabular result set. For example, `stats count by host` produces columns for `host` and `count`, with a row for each distinct host. When no grouping field is supplied, such as with `stats count`, it still returns a table containing the calculated field or fields. The command’s output is therefore structured data that can be displayed as a statistics table in Splunk Search. Users may subsequently select a visualization in the Search interface or configure one in a report or dashboard, but that visualization choice is separate from the result structure produced by the command itself. This table-oriented behavior also makes `stats` useful for summarizing large sets of events into counts, sums, averages, minimums, maximums, and other statistical calculations. Splunk’s command reference identifies `stats` as producing statistics from search results, while its reporting documentation describes statistics tables as a standard way to view transforming-command output. See the Splunk stats command documentation and Splunk statistical reporting documentation.

QUESTION NO: 3

You can also specify a time range in the search bar. You can use the following for beginning and ending for a

time range (Choose two.):

A. Not possible to specify time manually in Search query

B. end=

C. start=

D. earliest=

E. latest=

ANSWER: D E

Explanation:

`earliest=` and `latest=` are the SPL time modifiers used directly in the search bar to define the beginning and ending boundaries of a search time range. They can be supplied with relative time values, such as `earliest=-24h@h`, or with absolute timestamps, allowing a search to focus precisely on the events relevant to the investigation. For example, `index=main earliest=-7d latest=now` searches events from seven days ago through the current time. These modifiers are typically placed at the start of a search, alongside index and source restrictions, and they control the time interval Splunk uses when retrieving matching events. Splunk documents `earliest` as the lower time boundary and `latest` as the upper time boundary for searches. Time modifiers also support snapping with the `@` character, which is useful for reporting on complete hours, days, or other calendar periods. See the Splunk Search command reference and the Splunk documentation on time modifiers.

QUESTION NO: 4

Which of the statements are correct about HF? (Choose three.)

A. Parsing

B. Masking

C. Searching

D. Forwarding

ANSWER: A B D

Explanation:

A heavy forwarder (HF) is a full Splunk Enterprise instance configured primarily to receive, process, and forward data. **Parsing** is correct because, unlike a universal forwarder, a heavy forwarder can perform Splunk's parsing activities before it sends events onward. This processing includes interpreting incoming event data and applying index-time configuration where appropriate. **Masking** is also correct because a heavy forwarder can apply index-time transformations to redact or anonymize sensitive data before forwarding it. For example, administrators can use configured transforms or SEDCMD-based processing to remove or replace sensitive values as data passes through the heavy forwarder. **Forwarding** is correct because forwarding processed data to one or more indexers is the central role of this deployment type. This makes a heavy forwarder useful when data needs filtering, routing, transformation, or anonymization close to its source, while indexers retain responsibility for indexing the forwarded events. Splunk describes heavy forwarders as full Splunk Enterprise instances that can parse data and forward it to indexers. See Splunk documentation on forwarder types and Splunk documentation on anonymizing data.

QUESTION NO: 5

What options do you get after selecting timeline? (Choose four.)

A. Zoom to selection

B. Format Timeline

C. Deselect

D. Delete

E. Zoom Out

ANSWER: A B C E

Explanation:

Splunk's Search app timeline provides interactive controls for refining the displayed time range and adjusting how timeline results are presented. **Zoom to selection** is available after a time range is highlighted, allowing the selected interval to become the active search range. **Format Timeline** opens timeline-display settings, enabling users to control the timeline's presentation. **Deselect** removes the current highlighted time-range selection without applying it as a zoomed range. **Zoom Out** expands the currently displayed time window, making it possible to return to a broader view of event distribution over time. These controls support iterative investigation: users can identify an event spike or relevant period, focus on it, adjust the visualization, clear a selection when needed, and broaden the view again. Splunk documents the timeline as an interactive search-results visualization and describes using timeline selections to modify the displayed time range. See the Splunk Timeline search reference and Splunk's guidance on using the timeline in search.

QUESTION NO: 6

Which is a primary function of the timeline located under the search bar?

A. To differentiate between structured and unstructured events in the data

B. To sort the events returned by the search command in chronological order

C. To zoom in and zoom out. although this does not change the scale of the chart

D. To show peaks and/or valleys in the timeline, which can indicate spikes in activity or downtime

ANSWER: D

Explanation:

To show peaks and/or valleys in the timeline, which can indicate spikes in activity or downtime, is correct because the timeline is a visual histogram of the events returned by a search, distributed across the selected time range. Its primary value is helping an analyst quickly recognize how event volume changes over time. A pronounced peak can reveal a sudden increase in logged activity, such as a surge in errors, authentication attempts, traffic, or application requests. Conversely, a low point or gap can highlight an unusual reduction or absence of events, which may warrant investigation for service downtime, stopped logging, or a data-ingestion issue.

The timeline also supports interactive time-based investigation: selecting a portion of the histogram narrows the search to that interval, allowing the analyst to focus on the events responsible for an observed pattern. The histogram is therefore an immediate visual aid for identifying meaningful temporal patterns before drilling into individual events. Splunk documents the timeline as part of the Search page's event-viewing workflow and describes using it to investigate event distribution over time. See the Splunk Search Tutorial and the Splunk Timeline reference.

QUESTION NO: 7

Which search command is used to return events that contain a specified regular expression pattern?

A. regex

B. rexfield

C. match

D. pattern

ANSWER: A

Explanation:

`regex` is correct because it filters events using a regular expression applied to a field. For example, `| regex _raw="error|failed"` retains events whose raw text contains either pattern. See the Splunk regex command reference.

QUESTION NO: 8

Which of the following statements are correct about Search & Reporting App? (Choose three.)

A. Can be accessed by Apps > Search & Reporting.

B. Provides default interface for searching and analyzing logs.

C. Enables the user to create knowledge object, reports, alerts and dashboards.

D. It only gives us search functionality.

ANSWER: A B C

Explanation:

The Search & Reporting app is Splunk Enterprise's primary, built-in workspace for investigating indexed data. Users can open it from the Splunk platform's app menu by selecting *Apps* > *Search & Reporting*. Once in the app, its Search page provides the standard interface for entering SPL searches, selecting time ranges, reviewing events, examining fields, and using visualizations to analyze log and machine data. This makes it the default environment most users use to search and explore data.

The app also supports turning useful searches and analysis into reusable Splunk knowledge and operational content. A user can save searches, create reports that run on a schedule or on demand, define alerts from search results, and build dashboards that present search-based panels. These capabilities allow users to move from ad hoc investigation to repeatable monitoring, reporting, and shared visibility. Splunk documents the app as the place to search, analyze, and save searches, reports, alerts, and dashboards; see the Search & Reporting app overview and Splunk's knowledge objects documentation.

QUESTION NO: 9

Which all time unit abbreviations can you include in Advanced time range picker? (Choose seven.)

A. h

B. day

C. mon

D. yr

E. y

F. w

G. week

ANSWER: A C E F

Explanation:

The valid time-unit abbreviations represented in the supplied choices are `h`, `mon`, `y`, and `w`. Splunk's relative-time syntax, which is used by the Advanced time range picker, supports compact unit specifiers appended to an integer value, such as `-24h` for the previous 24 hours, `-1w` for the previous week, `-1mon` for the previous month, and `-1y` for the previous year. These abbreviations can also be combined with snapping operators where appropriate, for example `@w` to snap to the beginning of the current week. The Advanced picker accepts earliest and latest expressions based on this relative-time syntax, allowing users to define precise rolling or calendar-aligned search windows. The complete supported unit set also

includes seconds, minutes, days, and quarters, but their valid abbreviations are not fully represented by the supplied option text. See Splunk's Search time modifiers reference for the supported relative-time units and syntax, and the time modifier documentation for examples of earliest and latest time expressions.

QUESTION NO: 10

Splunk Enterprise is used as a Scalable service in Splunk Cloud.

A. True

B. False

ANSWER: A

Explanation:

True is correct. Splunk Cloud Platform is Splunk's cloud-based, software-as-a-service deployment of the Splunk platform. It provides the core search, analysis, dashboarding, alerting, and data-management capabilities associated with Splunk Enterprise while Splunk operates the underlying cloud infrastructure and much of the platform administration. This lets customers use Splunk's capabilities without deploying and maintaining their own Splunk Enterprise infrastructure.

Cloud delivery also supports scaling to meet an organization's data-ingestion, search, and user-access needs. Customers can select an appropriate Splunk Cloud Platform capacity and work with Splunk to adjust capacity as requirements grow. In this sense, Splunk Enterprise functionality is delivered through a managed, scalable cloud service rather than solely as a customer-managed on-premises installation. Splunk describes Splunk Cloud Platform as a SaaS solution for searching, monitoring, analyzing, and visualizing machine data, and its documentation explains the managed nature of the service. See the Splunk Cloud Platform overview and the Splunk Cloud Platform service documentation.

QUESTION NO: 11

When editing a dashboard, which of the following are possible options? (select all that apply)

A. Add an output.

B. Export a dashboard panel.

C. Modify the chart type displayed in a dashboard panel.

D. Drag a dashboard panel to a different location on the dashboard.

ANSWER: C

Explanation:

Modify the chart type displayed in a dashboard panel. is the correct single-choice answer. A Splunk dashboard panel is driven by a search and its visualization configuration. When a user edits a panel, Splunk provides visualization controls that let the user select an appropriate visualization type for the returned results, such as a column chart, line chart, area chart, pie chart, single value, table, or another supported visualization. This is a standard dashboard-authoring task: the underlying search can remain the same while the presentation is changed to make the results easier to interpret. For example, a time-based trend may be shown as a line chart, while grouped categorical results may be better presented as a bar or column chart. In Splunk Dashboard Studio, visualization type is configured through the visual editor and configuration panel; in classic dashboards, the visualization setting is available while editing the panel. The key principle is that a panel's search results and its visual representation are independently configurable, enabling authors to tailor dashboard displays to their monitoring or reporting needs. See Splunk's Dashboard Studio visualizations documentation and Splunk visualization documentation.

QUESTION NO: 12

Monitor option in Add Data provides _____.

A. Only continuous monitoring.

B. Only One-time monitoring.

C. None of the above.

D. Both One-time and continuous monitoring.

ANSWER: D

Explanation:

Both One-time and continuous monitoring. is correct because Splunk's Add Data workflow for files and directories supports two distinct collection behaviors. A one-time collection indexes the current contents of a specified file or directory and is useful for importing a static data set, such as an archived log file. Continuous monitoring configures Splunk to watch the specified path after the initial read, indexing new data as it is written to matching files. This is the normal approach for active application, system, and web-server logs.

These behaviors are configured as part of adding file and directory data inputs, allowing an administrator to select the collection method that fits whether the source is historical/static or actively changing. For continuously monitored inputs, Splunk tracks file position and uses its file-identification mechanisms to avoid repeatedly indexing data that it has already processed, while still collecting appended events. This flexibility is why the Add Data monitoring workflow covers both an initial, one-time ingestion use case and an ongoing monitoring use case. Splunk's documentation on monitoring files and directories and handling monitored log files provides the operational details.

QUESTION NO: 13

Which is the default app for Splunk Enterprise?

A. Splunk Enterprise Security Suite

B. Searching and Reporting

C. Reporting and Searching

D. Splunk apps for Security

ANSWER: B

Explanation:

The correct answer is **Searching and Reporting**. Splunk Enterprise includes the Search & Reporting app by default. This app is the primary workspace for users to search indexed data, save and run reports, create alerts, build dashboards, and work with knowledge objects such as fields, tags, event types, and lookups. When a user first accesses a standard Splunk Enterprise deployment, Search & Reporting is the default app context used for core data exploration and reporting workflows.

The app provides the main Search page and reporting capabilities that are fundamental to Splunk Enterprise usage, including SPL searches, result visualization, report scheduling, and dashboard creation. Its default availability is distinct from specialized premium solutions, which require separate installation and licensing. Splunk's documentation describes Search & Reporting as the app used to search data, create reports, and analyze results, and it is included with Splunk Enterprise. For additional detail, see the Splunk Search Tutorial and the Splunk Enterprise Admin Manual.

QUESTION NO: 14

You can on-board data to Splunk using following means (Choose four.):

A. Props

B. CLI

C. Splunk Web

D. savedsearches.conf

E. Splunk apps and add-ons

F. indexes.conf

G. inputs.conf

H. metadata.conf

ANSWER: B C E G

Explanation:

Splunk supports several supported paths for bringing data into an index. **CLI** is a valid onboarding method because administrators can use Splunk command-line commands, such as `splunk add monitor`, to create data inputs for files and directories. **Splunk Web** is also a standard method: the Add Data workflow provides guided configuration for common sources, including file and directory monitoring, network data, and scripted or modular inputs.

Splunk apps and add-ons provide another onboarding path. Add-ons commonly include preconfigured inputs, source types, field extractions, and knowledge needed to collect data from a specific technology, while apps can supply data-collection configurations and related workflows. **inputs.conf** is the primary configuration file for defining Splunk data inputs. Administrators can configure monitored files, TCP or UDP network inputs, scripted inputs, Windows inputs, and other input types in this file. These four methods can be used independently or together, depending on whether collection is configured interactively, through deployment-managed configuration, or through packaged integrations. See Splunk's Getting Data In documentation and the inputs.conf specification for supported input configuration details.

QUESTION NO: 15

Select the correct option that applies to Index time processing (Choose three.).

A. Indexing

B. Searching

C. Parsing

D. Settings

E. Input

ANSWER: A C E

Explanation:

Splunk index-time processing consists of the input, parsing, and indexing phases. **Input** is where Splunk receives data from configured sources such as files, network ports, or scripted inputs. During this phase, Splunk's input processors acquire the incoming data and pass it into the processing pipeline.

Parsing prepares the incoming stream for storage and search. Splunk identifies event boundaries, extracts or assigns timestamps, applies line breaking, and can assign or modify metadata such as host, source, and sourcetype. These actions are governed by relevant configuration settings, particularly in `props.conf`, and occur before the data is written to an index.

Indexing writes the processed events and their metadata to Splunk index files. Splunk creates searchable index structures, including the raw-data and index files that support efficient retrieval. Together, these phases describe how data moves from collection through event processing to persistent indexed storage. Splunk distinguishes these index-time activities from search-time processing, which occurs later when a user runs a search. See Splunk's How Splunk works overview and its indexing process documentation for the processing pipeline.

QUESTION NO: 16

In monitor option you can select the following options in GUI.

A. Only HTTP Event Collector (HEC) and TCP/UDP

B. None of the above

C. Only TCP/UDP

D. Only Scripts

E. Files & Directories, HTTP Event Collector (HEC), TCP/UDP and Scripts

ANSWER: E

Explanation:

Files & Directories, HTTP Event Collector (HEC), TCP/UDP and Scripts is correct because Splunk Web provides these as data-input methods in its graphical data onboarding and configuration workflows. File and directory monitoring lets a Splunk instance continuously read new data appended to specified files. TCP and UDP inputs allow Splunk to listen on network ports and receive events sent by external sources. HTTP Event Collector provides an HTTP or HTTPS endpoint through which applications and services can send event data directly to Splunk. Scripted inputs enable Splunk to run a script on a defined interval and index the output as events. These input types represent distinct ways to collect or receive machine data and are configurable through Splunk's data input interfaces, subject to the user's permissions and the deployment's configuration. Splunk's documentation describes file and directory monitoring as well as network and scripted data inputs in its data collection guidance, and documents HEC as a supported endpoint-based ingestion mechanism. See Splunk documentation: What Splunk can monitor and Splunk documentation: Use HTTP Event Collector.

QUESTION NO: 17

Data summary button just below the search bar gives you the following (Choose three.):

A. Hosts

B. Sourcetypes

C. Sources

D. Indexes

ANSWER: A B C

Explanation:

The Data Summary feature provides a high-level inventory of the data available to the current user in Splunk. It presents metadata-based views for **Hosts**, allowing users to see the systems sending events; **Sourcetypes**, which identify the format or category assigned to incoming events; and **Sources**, which identify the specific input path, file, network endpoint, or other origin from which events were collected. These views are useful before writing a search because they help a user discover what data is present and identify appropriate search constraints, such as `host=`, `sourcetype=`, or `source=`. The Data Summary is designed as a quick exploratory interface for these core event metadata fields, and its displayed values reflect data that the user is permitted to search. Splunk documents Data Summary as a way to examine hosts, sources, and source types in the indexed data. See the official Splunk documentation on using Data Summary and the metadata search command reference for related metadata concepts.

QUESTION NO: 18

Which statements are correct about using wildcards in Splunk searches? (Choose three.)

A. An asterisk can represent zero or more characters.

B. `host=web*` can match a host named web01.

C. `error*` can match a term beginning with error.

D. A wildcard always represents exactly one character.

E. Wildcards can only be used with numeric field values.

ANSWER: A B C

Explanation:

An asterisk (`*`) is a wildcard that can represent zero or more characters in a search term or field value. For example, `host=web*` can match hosts whose values begin with `web`, and `error*` can match terms that begin with `error`.

Wildcard searches can be useful when the complete value is not known, but broad wildcard searches can require more processing. Searches should use the most specific term possible. See the Splunk documentation on quick tips for searching.

QUESTION NO: 19

Search Language Syntax in Splunk can be broken down into the following components. (Choose all that apply.)

A. Search term

B. Command

C. Pipe

D. Functions

E. Arguments

F. Clause

ANSWER: A B D E F

Explanation:

Splunk Search Processing Language syntax is built from several core elements that combine to express a search and transform its results. A **Search term** identifies the events or field values to retrieve, such as a keyword, field-value pair, or index specification. A **Command** performs an action on the result set, including filtering, formatting, calculating, or aggregating data. **Functions** provide reusable calculations or evaluations within commands, particularly commands such as `eval`, `stats`, and `where`. **Arguments** supply the values, fields, expressions, and settings that tell a command or function how to operate. **Clause** refers to a syntactic portion of a command that modifies its behavior or organizes results, such as a grouping clause used with transforming commands. Together, these components let users construct searches ranging from simple event retrieval to detailed statistical analysis. Splunk's Search Reference documents command syntax, command arguments, and command-specific clauses, while the search manual describes how terms and commands form SPL searches. See the Splunk Search command reference and About the Search Processing Language.

QUESTION NO: 20

These users can create global knowledge objects. (Select all that apply.)

A. users

B. power users

C. administrators

ANSWER: B C

Explanation:

Power users and administrators can create knowledge objects with global sharing permissions. A globally shared knowledge object is available across all apps to users whose roles have the required permissions to access and use that object. This is appropriate for reusable items such as field extractions, event types, tags, lookups, reports, and data models that are intended to support searches beyond a single app context.

In Splunk's default role model, the power role provides expanded search and knowledge-object creation capabilities, including the ability to share eligible knowledge objects beyond the user's private context. The administrator role has broad management privileges and can likewise create and manage globally shared knowledge objects. Whether a particular object can be created or modified also depends on the relevant object-specific capabilities and permissions assigned to the role, but both of these default roles have the authority required for global sharing.

Global sharing should be used deliberately because globally available knowledge objects can affect search behavior across apps. Splunk recommends managing knowledge-object permissions according to the scope in which an object is needed. See Splunk's knowledge object permission documentation and its users and roles documentation for details.

QUESTION NO: 21

When editing a dashboard, which of the following are possible options? (Choose all that apply.)

A. Add an output.

B. Export a dashboard panel.

C. Modify the chart type displayed in a dashboard panel.

D. Drag a dashboard panel to a different location on the dashboard.

ANSWER: C

Explanation:

Modify the chart type displayed in a dashboard panel. is the correct answer. In Splunk dashboard editing, a panel's visualization can be configured independently of the underlying search. After selecting a panel in the dashboard editor, the author can use the visualization settings to choose how the returned results are presented, such as a column chart, bar chart, line chart, area chart, pie chart, single value, table, or other available visualization. This allows the dashboard author to adjust the display to make the same search results clearer and more useful for the intended audience without necessarily rewriting the SPL search. The selected visualization determines how Splunk interprets and renders the result set, while additional formatting and configuration settings can refine labels, colors, axes, legends, and similar presentation details. Splunk's dashboard documentation describes editing panels and configuring their visualizations as part of dashboard authoring, and its visualization documentation explains the available visualization types and their use with search results. See Splunk documentation on configuring visualizations and Splunk documentation on building and editing dashboards.

QUESTION NO: 22

Which searches correctly use the `stats` command? (Choose three.)

A. | stats count by host

B. | stats sum(bytes) by source

C. | stats avg(duration) as average_duration

D. | stats calculate bytes by host

E. | stats table host source

ANSWER: A B C

Explanation:

The `stats` command supports statistical functions such as `count`, `sum`, and `avg`. A `by` clause can be used to calculate the statistics separately for each value of one or more fields.

`| stats count by host` counts events for each host. `| stats sum(bytes) by source` calculates total bytes for each source. `| stats avg(duration) as average_duration` calculates an average and assigns a clearer output field name. See the stats command reference.

QUESTION NO: 23

Creating Data Models:

Fields associated with a data set are known as _____.

A. Attributes

B. Constraints

ANSWER: A

Explanation:

Attributes is correct because Splunk data models organize data into data sets, and each data set can have fields defined for it. Splunk calls the fields associated with a data set *attributes*. Attributes describe the information that the data set contains and make that information available for use when searching, reporting, and pivoting against the data model. For example, a data set representing web activity might have attributes such as client IP address, HTTP method, URI, status, and bytes transferred. Defining attributes gives a consistent field structure to the data represented by the data set, which is a key benefit of using a data model. The fields can be explicitly added to the data set and may be configured with field names, display names, and data types as appropriate. In the Data Model Editor, attributes are part of the data-set definition alongside the conditions that determine which events belong to that data set. Splunk's documentation describes data-model data sets as having constraints and fields, with those fields referred to as attributes. See Splunk's About data models and its Create data models guidance.

QUESTION NO: 24

Splunk Components:

Which of the following are responsible for reducing search results?

A. search heads

B. indexers

C. forwarders

ANSWER: A

Explanation:

Search heads are responsible for reducing search results in a distributed Splunk deployment. When a user runs a search, the search head coordinates that search across the relevant indexers. Each indexer searches its local data and returns intermediate or partial results. The search head then performs the reduce phase: it combines those distributed results, applies final search-processing commands and aggregations as needed, and presents the consolidated result set to the user. This map-and-reduce-style workflow allows Splunk to distribute work efficiently while still producing one coherent set of results for dashboards, reports, alerts, and ad hoc searches. For example, when a search uses transforming commands such as `stats`, indexers can calculate partial aggregations over their own data, and the search head merges those partial aggregations into the final values. Splunk documents that a search head distributes searches to indexers and merges the

returned results, which is the key responsibility described by reducing search results. See Splunk's documentation on search heads and the distributed search process.

QUESTION NO: 25

Three basic components of Splunk are (Choose three.):

A. Forwarders

B. Deployment Server

C. Indexer

D. Knowledge Objects

E. Index

F. Search Head

ANSWER: A C F

Explanation:

Splunk deployments are commonly described through three principal component roles: Forwarders, Indexer, and Search Head. Forwarders collect machine data from source systems and send it to Splunk indexers. This collection role allows data to be reliably transmitted from endpoints, servers, and applications without requiring users to perform searches on those systems. An Indexer receives the incoming data, parses it, stores it in indexes, and makes it available for efficient search. Indexing transforms raw event data into a form Splunk can search quickly. A Search Head provides the user-facing search and reporting experience. It distributes searches to indexers, combines returned results, and supports knowledge objects such as reports, dashboards, alerts, and field extractions. These roles can be installed on separate instances in distributed environments, while smaller installations may place more than one role on a single Splunk Enterprise instance. Together, Forwarders, Indexer, and Search Head represent the core flow of collecting, indexing, and searching data. Splunk's documentation describes these deployment roles and their responsibilities in its Splunk Enterprise components overview and distributed search documentation.

QUESTION NO: 26

Which of the following is an accurate definition of fields within Splunk?

A. Inherent entities that exist in event data.

B. A searchable key/value pair in event data.

C. Values pulled exclusively from lookup tables.

D. A non-searchable name/value pair used while indexing data.

ANSWER: B

Explanation:

A searchable key/value pair in event data is the accurate definition of a Splunk field. Splunk represents useful pieces of information in an event as a field name (the key) and its associated content (the value), such as `host=web01`, `status=200`, or `user=alex`. This structure lets users search, filter, group, calculate, and visualize event data based on meaningful attributes rather than treating every event solely as unstructured text. Fields can be extracted automatically at search time, identified through configured extractions, or added through knowledge objects such as lookups. Regardless of how a field is obtained, its key/value representation is what makes it available for SPL search commands and for use in the Fields sidebar. Splunk's documentation describes fields as searchable key-value pairs that are extracted from event data and used to refine searches and analyze results. This definition is central to Core Certified User skills because effective

searching commonly combines base search terms with field-based criteria, for example `index=main status=200`. See Splunk's documentation on fields and its Search Reference for field-based search syntax.

QUESTION NO: 27

Which statements are correct about the `eval` command? (Choose three.)

A. It can create a new field.

B. It can replace the value of an existing field.

C. It can use functions and operators in expressions.

D. It always removes the original event data.

E. It groups events by field values.

ANSWER: A B C

Explanation:

The `eval` command is used to calculate an expression and store the result in a field. It can create a new field, such as `| eval total=price*quantity`, and it can replace the value of an existing field. It also supports evaluation functions and operators for calculations, text processing, conditional logic, and date and time handling.

The `eval` command does not aggregate results into groups; commands such as `stats` perform that function. See the Splunk documentation for the eval command.

QUESTION NO: 28

Which of the following statements describes a search job?

A. Once a search job begins, it cannot be stopped

B. A search job can only be paused when less than 50% of events are returned

C. A search job can only be stopped when less than 50% of events are returned

D. Once a search job begins, it can be stopped or paused at any point in time

ANSWER: D

Explanation:

Once a search job begins, it can be stopped or paused at any point in time. In Splunk, every search that runs creates a search job, which has a job identifier and a lifecycle that can be managed from the Search & Reporting interface or through Splunk's search-job management endpoints. While a job is running, a user can pause it to temporarily suspend processing. Pausing is useful when an analyst wants to preserve the current job and its partial results while deferring further resource consumption. The job can subsequently be resumed so that Splunk continues processing the same search. A running job can also be stopped when it is no longer needed; stopping ends the job rather than requiring it to run to its natural completion. These controls are available during execution and are not contingent on a particular percentage of returned events. Splunk also exposes job state and management capabilities through the REST API, including actions for controlling active search jobs. For more detail on search job concepts and management, see Splunk Search Manual: About jobs and job management and Splunk REST API Reference: search jobs.

QUESTION NO: 29

Matching search terms are highlighted.

A. Yes

B. No

ANSWER: A

Explanation:

Yes is correct. In Splunk Search, matching search terms are highlighted in the event data shown on the Events tab. This visual treatment helps analysts quickly locate the portions of each returned event that caused it to match the search, rather than manually scanning the full raw event text. Highlighting is especially useful when a search returns many long events, because it provides an immediate visual connection between the search criteria and the matching fields or values in the results. Splunk's search-results interface is designed to support examination of individual events, including displaying matching terms in the event list. The highlighting behavior applies to the search terms used to retrieve the events and assists with rapid validation and investigation of search results. For further details about examining search results and working with events in Splunk Search, see the Splunk Search Tutorial: Examine your search results and the Splunk Search Reference.