Quizlet

Splunk Core Certified User & Splunk Fundamentals 1

Terms in this set (237)

T/F: Machine data is always structured.	False. Machine data can be structured or unstructured.
Machine data makes up for more than __% of the data accumulated by organizations.	90

T/F: Machine data is only generated by web servers.	False
Search requests are processed by the _____.	Indexers
Search strings are sent from the _____.	Search Head
In most Splunk deployments, _____ serve as the primary way data is supplied for indexing.	Forwarders

Which of these is **not** a main component of Splunk? A) Search and investigate. B) Compress and archive. C) Add knowledge. D) Collect and index data.	B) Compress and archive
What are the three main processing components of Splunk? **(Select all that apply.)** A) Indexers B) Deployment Maker C) Search Heads D) Forwarders E) Distributors	A) Indexers C) Search Heads D) Forwarders
_____ define what users can do in Splunk. A) Tokens B) Disk permissions C) Roles	C) Roles
This role will only see their own knowledge objects and those that have been shared with them. A) User B) Power C) Admin	A) User

T/F: You can launch and manage apps from the home app.	True
What are the three main default roles in Splunk Enterprise? **(Select all that apply.)** A) King B) User C) Manager D) Admin E) Power	B) User D) Admin E) Power
Which apps ship with Splunk Enterprise? **(Select all that apply.)** A) Home App B) Sideview Utils C) Search & Reporting D) DB Connect	A) Home App C) Search & Reporting
The default username and password for a newly installed Splunk instance is: A) username and password B) admin and changeme C) admin and 12345 D) buttercup and rawks	B) admin and changeme

Files indexed using the **upload** input option get indexed ____. A) Each time Splunk restarts. B) Every hour. C) On every search. D) Once.	D) Once.
T/F: The monitor input option will allow you to continuously monitor files.	True
Splunk knows where to break the event, where the time stamp is located and how to automatically create field value pairs using these. A) Line breaks B) Source types C) File names	B) Source types
Splunk uses _____ to categorize the type of data being indexed.	sourcetype
In most production environments, _____ will be used as your the source of data input.	Forwarders

How is the **asterisk** used in Splunk search? A) As a wildcard. B) To make a nose for your clown emoticon. C) As a place holder. D) To add up numbers.	A) As a wildcard.
Which following search mode toggles behavior based on the type of search being run? A) Smart B) Fast C) Verbose	A) Smart
T/F: When zooming in on the event time line, a new search is run.	False

T/F: These searches will return the same results... failed password failed AND password	True

Splunk Core Certified User & Splunk Fundamentals 1

A search job will remain active for ____ minutes after it is run. A) 5 B) 10 C) 30 D) 60 E) 90	B) 10
What attributes describe the field below? a dest 4 (Select all that apply.) A) It contains 4 values. B) It contains numerical values. C) It cannot be used in a search. D) It contains string values.	A) It contains 4 values. D) It contains string values.
T/F: Wildcards cannot be used with field searches.	False
T/F: Field values are case sensitive.	False

Splunk Core Certified User & Splunk Fundamentals 1

Which is not a comparison operator in Splunk? (Select your answer.) A) > B) ?= C) <= D) != E) =	?=
Field names are _____. **(Select all that apply.)** A) Always capitalized. B) Not important in Splunk. C) Case sensitive. D) Case insensitive.	C) Case sensitive
This symbol is used in the "Advanced" section of the time range picker to round down to nearest unit of specified time. (Select your answer.) A) % B) ^ C) @ D) & E) *	C) @
T/F: Time to search can only be	False

What is the most efficient way to filter events in Splunk? A) By time. B) Using booleans. C) With an asterisk.	A) By time.
T/F: As a general practice, exclusion is better than inclusion in a Splunk search.	False
Having separate indexes allows: **(Select all that apply.)** A) Faster Searches. B) Ability to limit access. C) Multiple retention policies.	A) Faster Searches. B) Ability to limit access. C) Multiple retention policies.

Would the ip column be removed in the results of this search? Why or why not? sourcetype=a* | rename ip as "User" | fields - ip A) Yes, because a pipe was used between search commands. B) No, because the name was changed. C) No, because table columns can not be removed. D) Yes, because the negative sign was used.	B) No, because the name was changed.
T/F: Excluding fields using the Fields Command will benefit performance.	False
Which command removes results with duplicate field values? A) Dedup B) Limit C) Join D) Distinct	A) Dedup

What is missing from this search?... sourcetype=a* | rename ip as "User IP" | table User IP A) A pipe. B) Search terms C) Quotation marks around User IP. D) A table command.	C) Quotation marks around User IP.
What command would you use to **remove the status field** from the returned events? sourcetype=a* status=404 | _____ status A) table B) fields - C) not D) fields	B) fields -
Which one of these is not a stats function? A) Count B) Avg C) Addtotals D) List E) Sum	C) Addtotals

Splunk Core Certified User & Splunk Fundamentals 1

To display the most common values in a specific field, what command would you use? A) top B) all C) table D) rare	A) top
Which clause would you use to rename the count field? sourcetype=vendor* | stats count _____ "Units Sold" A) rename B) to C) as D) show	C) as

How many results are shown by default when using a Top or Rare Command?	10
Which stats function would you use to find the average value of a field?	average (or avg)

Splunk Core Certified User & Splunk Fundamentals 1

If a search returns this, you can view the results as a **chart**. A) A list. B) Statistical values C) Time limits. D) Numbers	B) Statistical values
T/F: A time range picker can be included in a report.	True
These roles can create reports: **(Select all that apply.)** A) Admin B) User C) Power	A) Admin B) User C) Power
In a dashboard, a time range picker will only work on panels that include a(n) _____ search. A) transforming B) inline C) visualization D) accelerated	B) inline
T/F: The User role can not create reports.	False

Adding child data model objects is like the _____ operator in the Splunk search language. A) NOT B) AND C) OR	B) AND
T/F: Pivots cannot be saved as reports panels.	False
The instant pivot button is displayed in the statistics and visualization tabs when a _____ search is run. A) transforming B) non-transforming	B) non-transforming

These are knowledge objects that provide the data structure for pivot. A) Alerts B) Indexes C) Reports D) Data models	D) Data models
T/F: Pivots can be saved as dashboards panels.	True

T/F: A lookup is categorized as a dataset.	True
External data used by a Lookup can come from sources like: **(Select all that apply.)** A) Scripts. B) CSV files. C) None. Only internal data can be used. D) Geospatial data.	A) Scripts B) CSV files D) Geospatial data
When using a .csv file for Lookups, the first row in the file represents this. A) Field names. B) Output fields. C) Nothing, it is ignored. D) Input fields.	A) Field names.
Finish this search command so that it displays data from the http_status.csv Lookup file. | _____ http_status.csv A) inputlookup B) lookup=* C) datalookup D) lookup	A) inputlookup

To keep from **overwriting** existing fields with your Lookup you can use the _____ clause.	OUTPUTNEW
T/F: Alerts can be shared to all apps.	True
T/F: Real-time alerts will run the search continuously in the background.	True
T/F: Alerts can run uploaded scripts.	True
T/F: Once an alert is created, you can no longer edit its defining search.	False
T/F: Alerts can send an email.	True
Which function is not a part of a single instance deployment? A) Searching B) Parsing C) Clustering D) Indexing	C) Clustering

T/F: Events are always returned in chronological order.	False
Finish the rename command to change the name of the status field to HTTP Status. sourcetype=a* status=404 | rename _____ A) as "HTTP Status" B) status as "HTTP Status" C) status to "HTTP Status" D) status as HTTP Status	B) status as "HTTP Status"
_____ are reports gathered together into a single pane of glass. A) Dashboards B) Panels C) Alerts D) Scheduled Reports	A) Dashboards
An alert is an action triggered by a _____. A) Selected field B) Tag C) Report D) Saved search	D) Saved Search

What is a transforming command?	A type of search command that **orders the results into a data table**. Transforming commands "transform" the specified cell values for each event into numerical values that Splunk Enterprise can use for statistical purposes.
What are **seven** common transforming commands?	Transforming commands include: 1) chart 2) timechart 3) stats 4) top 5) rare 6) contingency 7) highlight.
What does CIM stand for and what is it?	Common Information Model (CIM). A shared semantic model focused on extracting value from data. The CIM is implemented as an add-on that contains a collection of data models, documentation, and tools that support the consistent, normalized treatment of data for maximum efficiency at search time.
What is a lookup?	Lookup is a command to **invoke field value lookups**. The lookup command can merge unstructured and structured data For example: ...l lookup <lookup-table-name> <lookup-field1> AS <event-field1>

What is a scheduled report?	A report that is scheduled to run on a regular interval, making it a type of **scheduled search**. Scheduled reports typically initialize one or more alert actions each time they run, such as sending the results of the report run to a set of recipients, logging and indexing custom log events, or adding the results to a CSV lookup.
What is pivot?	Pivot is a command that applies a pivot operation to data. For example: This command counts the number of events in the "HTTP Requests" object in the "Tutorial" data model. ...| pivot Tutorial HTTP_requests count(HTTP_requests) AS "Count of HTTP requests"
What are the **three** required parts of a pivot?	The pivot command is a generating command and must be first in a search pipeline. It requires a large number of inputs: **the data model**, **the data model object**, and **pivot elements**. ...| pivot <datamodel-name> <object-name> <pivot-element>
What does SPL stand for and what are some of it's features?	Search Processing Language (SPL) It is Splunk's **proprietary** language. SPL encompasses all the search commands and their functions, arguments, and clauses. Its syntax was originally **based on the Unix pipeline and SQL**. The scope of SPL includes **data searching, filtering, modification, manipulation, insertion, and deletion**.

What is the most recent version of Splunk that is stable?	Spunk Version 7.2.1 (As of 12/06/2018)
What are the **three** Splunk search modes?	1) **Verbose** (returns most amount of data) 2) **Fast** (limits types of data returned and emphasizes speed) 3) **Smart** (switches to verbose or fast based on search)
How would you use a wildcard to create a search that looks for all of the **product IDs** that begin with the letter **S** and end in **G01**.	productID=S*G01
Indexes consist of what **two** types of files?	1) Raw data files 2) Index files
What is an index?	A collection of databases.
What is time-series data?	Any data with time stamps.
How does Splunk indexing work?	Time-series data is broken into events, based on the timestamps.

Splunk Core Certified User & Splunk Fundamentals 1

When should you avoid using wildcards?	When the items searched against have **punctuation**, such as SF-RT_5G01 A typical search would be: productID=S*G01 But due to the way Splunk indexes punctuation (such as underscore or dash), this search would likely fail.
What is the difference between **stats**, **chart**, and **time chart**?	Stats: Tabular format that allows **unlimited fields**. Chart: Graphical format that allows **two fields** (x and y axis) and can be pie chart, bar chart, line chart etc. Time Chart: Allows display in bar or line graph format, and only takes in **one field** because it uses time for the X axis.
What are the **five** default fields for every event in Splunk?	1) host 2) source 3) source type 4) index 5) timestamp
All of Splunk's configurations are written within what file type?	Plain text **.conf** files.
What are the **five** Splunk data bucket ages, from most current to oldest?	1) Hot 2) Warm 3) Cold 4) Frozen 5) Thawed
What happens to data once it	Depending on the aging policy, the data in the

What does a Splunk license specify?	How much **data** you can index per calendar day.
What does a generating command do?	A generating command **fetches information** from the indexes, **without any transformations**. Generating commands are either event-generating (distributable or centralized) or report-generating. Most report-generating commands are also centralized. Depending on which type the command is, the results are returned in a list or a table.
What does the metadata command do?	The metadata command returns a list of sources, sourcetypes, or hosts from a specified index or distributed search peer. For Example: ...| metadata type=hosts
What is the Splunk data inspector process?	1) Look at data and decide how to process it. 2) Label data by source type. 3) Break data into events. 4) Normalize timestamps. 5) Added to Splunk index to be searched
Where would you go to determine whether the built-in search optimizations are helping your search to complete faster?	Job Inspector
What is the job of the Search Head?	**Handle search requests** using Splunk search language. Enriches data with reports, dashboards, visualizations.

Search heads send searches to...	Indexers
What processes machine data, storing the results in indexes as events, and enables fast search and analysis?	The Splunk **Indexer**.
As the Indexer indexes data, it creates a number of files organized by _____	age (using the imestamps)
What do Indexes point to?	Indexes point to raw compressed data.
Which Splunk component allows a user to extract fields and transform data without changing the underlying index data?	Search Heads
Where do forwarders usually reside?	Forwarders reside on the machines where the data originates.
Which Splunk component supplies data to be indexed?	Forwarders
What are the three less common Splunk components?	1) Deployment Server 2) Cluster Master 3) License Master
What are the Splunk **Basic** Deployment limitations?	1) Indexing less than 20GB per day. 2) Under 20 users. 3) Limited number of forwarders.

What is the minimum number of search heads required for a search head cluster?	Three
What is used to **manage and distribute apps** to the members of the search head cluster?	A deployer.
What are the benefits of a Search Head Cluster?	1) Services more users. 2) Allows users and searches to share resources. 3) Distribute requests across the set of indexers.
What are the benefits of a traditional Index Cluster?	1) Replicate data. 2) Prevent data loss. 3) Promote availability. 4) Manage multiple indexers.
Which ports are required for Splunk?	1) splunkweb, port 8000 2) splunkd, port 8089 3) forwarder, port 9997
What does the *NIX command do for a Splunk installation?	*NIX decompresses the .tar.gz file in the path you want Splunk to run from.
What file extension is the Windows installer?	.msi
While Splunk starts automatically on Windows after installation, to automatically start Splunk on a Linux a user is required to enable...	boot-start

The difference between a single deployment and an Splunk enterprise deployment is in...	The post-deployment configuration.
Which CLI command is used to... **Display a command usage summary**	splunk help
Which CLI commands are used to... **Manage the Splunk processes**	splunk [start | stop | restart] <process_name>
Which CLI command is used to... **Automatically accept the license without prompt**	splunk start --accept-license
Which CLI command is used to... **Display the Splunk process status**	splunk status
Which CLI command is used to... Show the port that the **splunkd** listens on	splunk show splunkd-port

Which CLI command is used to... Show the port that **Splunk Web** listens on	splunk show web-port
Which CLI command is used to... **Show the servername of this instance**	splunk show servername
Which CLI command is used to... **Show the default host name used for all data inputs**	splunk show default-hostname
Which CLI command is used to... **Initialize script to run Splunk Enterprise at system startup**	splunk enable boot-start -user
Users with the account type _____ can create additional roles and create apps.	administrator
What is the **URL** used by administrators for creating and installing additional Splunk apps?	splunkbase.splunk.com
What are the **three** options	1) Upload 2) Monitor

In what circumstance might you use the **upload** option for app data?	When **testing** OR when searching small data sets that are **not updated**.
In the following sample device log entries, which parts are the field names, field values, and delimiters?... icmp_seq=0 ttl=64	Field names: icmp_seq and ttl Field values: 0 and 64 Delimiters: equal signs "="
When Splunk does not have a predefined way to **break events**, how does is it accomplish the task?	Either through **time stamps** or **regular expressions**.
What happens if the forwarder to indexer connection is lost?	Splunk will queue the input data and once the connection is reestablished, Splunk will begin sending data from where it left off.
In regards to the Data Summary window, what is the difference between: Host, Source, and Sourcetype?	**Host**: A semi-unique identifier, such as host name, IP address, etc. **Source**: Name of the file, stream, path, etc. **Sourcetype**: The product or software type, such as cisco_asa, ps, win_audit, etc.
Every report and visualization is built based on _____.	an underlying search.
What is the benefit of using a monitor over a forwarder?	A monitor sends event data as it happens, rather than on a schedule, allowing near real time information.

For production environments what are the main source of data input?	Forwarders
Which boolean operator is implied between search terms?	AND
Are search terms case sensitive?	No. While field names are case sensitive, search terms are case **insensitive**.
Searching **exact phrases**, such as **best effort** or **unit 0837** require the use of what?	Quotation marks, i.e. ... "best effort" or "unit 0837"
Which default automated tool provides selections for how to complete the search string?	Search Assistant
What are the two Search Assistant modes?	1) Compact 2) Full
In what order are search results returned?	Reverse chronological order, i.e. newest first.
T/F: Matching search terms are highlighted.	True
When Splunk parses data into individual events, each event typically includes which **four** fields?	1) timestamp 2) host 3) source 4) sourcetype

What is the name of the tab that displays possible field choices on the left of the search results screen?	The Fields Sidebar
If you click a highlighted keyword from search results, what are the three options you are given?	1) Add to search 2) Exclude from search 3) New Search
What are the **three** search result view options?	1) List (default) 2) Table 3) Raw
What are the **six** time range tabs in the time picker drop down menu?	1) Presets (default) 2) Relative 3) Real-time 4) Date Range 5) Date & Time Range 6) Advanced
What is the search results timeline used for?	The search results timeline **displays the distribution of the event results** and can be used to **drill into specific time ranges** of interest.
What are Splunk jobs typically tied to?	Searches
What is the default time search jobs are available for?	10 minutes

What are the **three** ways can you share a particular search you've created?	In the bottom right of the search bar there are **job options**, which allow you to do the following: 1) Obtain a sharable **link** for the search/results. 2) **Print** the Search results. 3) Save the search results as a **PDF**.