Quizlet

Splunk Fundamentals 1

Terms in this set (65)

Machine data is only generated by web servers.	False
Machine data makes up for more than __% of the data accumulated by organizations.	90
Machine data is always structured.	False
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? Search and investigate Compress and archive Add knowledge Collect and index data	Compress and Archive

Which function is not a part of a single instance deployment? Clustering Parsing Indexing Searching	Clustering
A single-instance deployment of Splunk Enterprise handles: Select all that apply. Indexing Parsing Input Searching	Indexing Parsing Input Searching
What are the three main default roles in Splunk Enterprise? Select all that apply. User Power User Administrator Manager King	User Power User Administrator

Which apps ship with Splunk Enterprise? Select all that apply. Home App Search & Reporting DB Connect Sideview Utils	Home App Search & Reporting
______ define what users can do in Splunk. Tokens Roles Disk permissions	Roles
The password for a newly installed Splunk instance is: Your email address. Available from the splunk.com website. Randomly generated. Created when you install Splunk Enterprise.	Created when you install Splunk Enterprise.

You can launch and manage apps from the home app.	True
Splunk uses _____ to categorize the type of data being indexed.	sourcetypes

Splunk knows where to break the event, where the time stamp is located and how to automatically create field value pairs using these. Line breaks File names Source types	sourcetypes
The monitor input option will allow you to continuously monitor files.	True
Files indexed using the the upload input option get indexed ___. Each time Splunk restarts Every hour On every search Once	Once
In most production environments, ____ will be used as your main source of data input.	Forwarders
When a search is sent to splunk, it becomes a ___. File on the host system Task for Jimmy the Splunk elf Search job Event	Search job

Shared search jobs remain active for _____ by default. 24 hours 1 year 10 minutes 1 day 7 days	7 Days
A search job will remain active for __ minutes after it is run. 10 90 5 30 20	10 Minutes
Which following search mode toggles behavior based on the type of search being run? Fast Smart Verbose	Smart

What is the order of evaluation for Boolean operations in Splunk?	NOT - OR - AND

What attributes describe the circled field below? "a dest 4" Select all that apply It contains string values. It cannot be used in a search. It contains 4 values. It contains numerical values	It contains string values It contains 4 values
Which is not a comparison operator in Splunk? > ?= != = <=	?=
Field names are _____. Select all that apply. Case insensitive Always capitalized Not important in Splunk Case sensitive	Case sensitive
Field values are case sensitive.	False
Wildcards cannot be used with field searches.	False

What is the most efficient way to filter events in Splunk? By time. Using booleans. With an asterisk.	By time
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. & @ ^ * %	@
Time to search can only be set by the time range picker	False
Having separate indexes allows: Select all that apply. Multiple retention policies Ability to limit access. Faster Searches.	Multiple retention policies Ability to limit access Faster Searches

As a general practice, exclusion is better than inclusion in a Splunk search.	False
What command would you use to remove the status field from the returned events? "sourcetype=a* status=404 | ______ status not fields table fields -	fields -
Excluding fields using the Fields Command will benefit performance.	False
What is missing from this search? "sourcetype=a* | rename ip as "User IP" | table User IP A table command Search terms A pipe Quotation marks around User IP	Quotation marks around User IP

Finish the rename command to change the name of the status field to HTTP Status

"sourcetype=a* status=404 | rename _______"

status as "HTTP Status"
status to "HTTP Status"
as "HTTP Status"
status as HTTP Status

status as "HTTP Status"

Would the ip column be removed in the results of this search? Why or why not?

"sourcetype=a* | rename ip as "User" | fields - ip"

Yes, because the negative sign was used.
No, because table columns can not be removed.
Yes, because a pipe was used between search commands
No, because the name was changed.

No, because the name was changed.

Which clause would you use to rename the count field? "sourcetype=vendor* | stats count _____ "Units Sold"" to as rename show	As
To display the most common values in a specific field, what command would you use? top rare table all	Top
Which stats function would you use to find the average value of a field?	Avg
Which one of these is not a stats function? Count Addtotals Avg Sum List	Addtotals

How many results are shown by default when using a Top or Rare Command?	10
Charts can be based on numbers, time, or location	True
The User role can not create reports	False
Question : 3 A time range picker can be included in a report	True
________ are reports gathered together into a single pane of glass. Alerts Panels Dashboards Scheduled Reports	Dashboards
If a search returns this, you can view the results as a chart Time limits. Numbers A list. Statistical values	Statistical values

These are knowledge objects that provide the data structure for pivot. Indexes Data models Alerts Reports	Data models
Pivots cannot be saved as reports panels	False
Adding child data model objects is like the ____ Boolean in the Splunk search language	AND
Data models are made up of _______. Datasets Dashboard panels Transforming searches Pivots	Datasets

Pivots can be saved as dashboards panels	True
The instant pivot button is displayed in the statistics and visualization tabs when a _____ search is run.	Non-transforming

Which role(s) can create data models? Select all that apply. Power User Administrator User	Power User Administrator
External data used by a Lookup can come from sources like: Select all that apply. None. Only internal data can be used. CSV files Geospatial data Scripts	CSV files Geospatial data Scripts
Finish this search command so that it displays data from the http_status.csv Lookup file " I _____ http_status.csv" lookup=* datalookup lookup inputlookup	inputlookup

When using a .csv file for Lookups, the first row in the file represents this. Nothing, it is ignored Output fields Input fields Field names	Field names
To keep from overwriting existing fields with your Lookup you can use the _______ clause.	OUTPUTNEW
A lookup is categorized as a dataset	True
Alerts can run uploaded scripts.	True
Real-time alerts will run the search continuously in the background.	True
An alert is an action triggered by a ________. Selected field Tag Saved search Report	Saved search
Once an alert is created, you can no longer edit its defining search	False

Alerts can send an email.	True