**Intro to Splunk (100%)**

1. What are the default roles in Splunk Enterprise?

* **User**
* **Power**
* **Admin**

1. Which of the following searches will return results containing the words fail, failure, or failed?

**Fail\***

1. Which search mode behaves differently depending on the type of search being run?

**Smart**

1. What determines the timestamp shown on returned events in a search?

**The time zone defined in user settings**

1. Which Splunk infrastructure component stores ingested data?

**Index**

1. By default, how long does a search job remain active?

**10 minutes**

1. When a search is run, in what order are events returned?

**Reverse chronological order**

1. By default, which of the following roles are required to share knowledge objects?

* **Power**
* **Admin**

1. Which of the following searches will return results containing the terms failed, password, or failed password?

* **Failed OR password**
* **Failed OR password OR “failed password”**

1. Which of the following booleans can be used in a search?

* **NOT**
* **OR**
* **AND**

1. Which command can be used to further filter results in a search?

**Search**

1. Which character is used in a search before a command?

**A pipe (|)**

1. What is the most efficient way to limit search results returned?

**Time**

1. By default, who is able to view a saved report?

**The user who created it**

**Using Fields (100%)**

1. At search time, if an event has an equal(=) sign, the data to the left is treated as a \_\_\_\_\_\_ and the data to the right is treated as a \_\_\_\_\_\_.

**Field name, value**

1. Which of the following fields are default selected fields?

* **Host**
* **Source**
* **Sourcetype**

1. The fields command allows you to do which of the following? Select all that apply.

* **Include fields (fields)**
* **Include fields (fields +)**
* **Exclude fields (fields -)**

1. In the Fields sidebar, Interesting Fields occur in at least \_\_\_\_\_\_\_\_ of resulting events.

**20%**

1. To remove fields from a search, you would use the \_\_\_\_\_\_\_\_\_ command.

**fields –**

1. True or False: Once you rename a field, the new field name must be used in the rest of the search string.

**True**

1. At search time, \_\_\_\_\_\_\_ extracts fields from raw event data.

**Field discovery**

1. True or False: Fields are knowledge objects.

**True**

**Scheduling Reports & Alerts (93%)**

1. Which alert action allows you to send an event to your Splunk deployment for indexing?

**Log event**

1. Which alert setting allows you to control how many alert actions are taken when trigger conditions are met?

**Throttle**

1. Which Edit setting allows a report to be displayed to users outside of your organization?

**Embed**

1. What is a primary benefit of scheduling reports?

**Scheduling a report reduces the demand that concurrently running reports can put on your system hardware.**

1. Which of the following user roles are able to display a report in all apps?

**All options are wrong, WTF SPLUNK, (Admin or the user who created the app)**

1. Which alert action allows you to send a message to an external chat room?

**Webhook**

1. Which of the following user roles are able to display a report in the app in which it was created?

* **Admin**
* **Power**

1. Which scheduled report setting helps determine when concurrent reports will run?

**Schedule priority**

1. Which scheduled alert type will continuously run in the background?

**Real-time**

1. Which scheduled report setting allows you to define a time range for a report to run if it is delayed?

**Schedule window**

1. Select the two valid types of alerts.

* **Real-time**
* **Scheduled**

1. When are actions triggered for a real-time alert?

**As soon as alert conditions are met**

1. If a dashboard panel is powered by a scheduled report, how frequently will its contents update?

**The dashboard panel updates based on the underlying report's scheduling settings.**

1. Which of the following prebuilt alert actions can be triggered when a report is run?

* **Output results to a lookup**
* **Send an email**

**Visualizations (100%)**

1. Which optional argument of the addtotals command changes the label for row totals in a table?

**Fieldname**

1. In a single series data table, which column provides the x-axis values for a visualization?

**The first column**

1. Which argument can be used with the timechart command to specify the time range to use when grouping events?

**Span**

1. Which clause can be used with the top command to specify a number of values to return?

**Limit**

1. Which type of default map visualization uses shading to represent relative metrics?

**Choropleth Map**

1. Which of the following commands can return a count of all events matching search criteria over a specified time period?

**Stats**

1. Which command removes duplicate field values in search results?

**Dedup**

1. Which clause can be used with the rare command to specify whether or not a percentage column is created?

**Showperc**

1. When using the timechart command, which axis represents time?

**X-axis**

1. How can the order of columns in a table be changed?

**By changing the order of fields specified in the table command**

1. Which command can be used to exclude fields from search results?

**Fields**

1. Which command changes the appearance of field values?

**Fieldformat**

1. Which clause can be used with the top command to change the name of the count column?

**Countfield**

1. Which argument can be used with the geostats command to control the column count?

**Globallimit**

1. How many columns are displayed in a visualization by default when using the chart command?

**10**

**Search Under the Hood (100%)**

1. When is a bucket's bloom filter created?

**When a bucket rolls from hot to warm**

1. After Splunk tokenizes terms at index time, where are the tokens stored?

**In the lexicon**

1. If a search begins with a distributable streaming command, where is it first executed?

**On the indexer**

1. Which component of a bucket stores raw event data?

**Journal**

1. Where can comments be placed in a search?

**Comments can be placed anywhere inside a search**

1. Where should the makeresults command be placed within a search?

**The makeresults command must be the first command in a search**

1. Which of the following conditions could cause a lispy expression to not create tokens?

**A wildcard at the beginning of a search**

1. Which of the following commands generates temporary search results?

**Makeresults**

1. Which of the following syntaxes signify a comment in SPL?

**```comment```**

1. Which architectural component of a Splunk deployment initiates a search?

**Search Head**

1. Which of the following expressions builds a search-time bloom filter?

**A lispy expression**

1. Which component of the Search Job Inspector shows how long a search took to execute?

**Header**

1. Which directive can be used in a search to bypass minor breakers inside the supplied argument?

**TERM**

1. Where in the search pipeline are transforming commands executed?

**On the search head**

1. Which of the following breakers would be used first in segmentation?

**Commas**

**Intro to Knowledge Objects (100%)**

1. When a user has left your organization, what happens to their knowledge objects?

**An admin can reassign them to another user**

1. Which knowledge object type can communicate with external sources using the HTTP GET and POST methods?

**Workflow actions**

1. Which two of the following knowledge object types can contain an eval expression?

* **Calculated fields**
* **Macros**

1. Which knowledge object type can contain an eval expression?

**Calculated fields**

1. Which of the following file types can be uploaded to create a lookup?

**CSV**

1. Where can you find a list of all fields returned from events?

**The fields sidebar**

1. Which of the following user roles can create knowledge objects?

* **Admin**
* **Power User**
* **User**

1. By default, what user role is required to make a knowledge object available to all apps?

**Admin**

1. Which knowledge object type can be searched in Pivot?

**Data models**

1. Which of the following methods can be used to manually extract fields?

* **Regular Expressions, or RegEx**
* **Delimiters**

1. Which knowledge objects can be scheduled to execute at specific times?

* **Reports**
* **Alerts**

1. By default, when a knowledge object is created, who can access its contents?

**The user who created it or a user with an admin role**

1. Which knowledge object type can store entire search strings, including commands?

**Macros**

1. What are the three predefined sharing options for a knowledge object?

* **Shared in app**
* **Shared in all apps**
* **Private**

1. What are the primary functions of a workflow action?

* **Communicating with an external source using the HTTP POST method**
* **Communicating with an external source using the HTTP GET method**
* **Passing information back to Splunk to run a secondary search**

**Getting Data Into Splunk (100%)**

1. In almost all production Splunk environments, most of the input data comes from which Splunk components?

**Forwarders**

1. If a data input is created in the Splunk Web interface with an App Context set to Search & Reporting (search), where will the configuration files be stored for this input?

**SPLUNK\_HOME/etc/apps/search/local**

1. Which of the following is not a supported Splunk data input types?

**Executable files**

1. What is the default index where Splunk will store event data, if an alternative is not specified?

**main**

1. Which of the following Linux-specific source types is provided in the Splunk Web interface?

**Systemd Journald Input**

1. Splunk will not update an inputs.conf file when you use which of the following:

**The Upload option in Settings > Add Data**

**Splunk Enterprise Installation and Configuration**

1. Which of the following configures Splunk to boot-start automatically?

**Windows Only**

1. What is the default installation path for Splunk (also known as SPLUNK\_HOME) on Linux?

**/opt/splunk**

1. Which of the following port numbers is associated with the splunkd process by default?

**8089**

1. Which installer is used to install a Splunk Search Head?

**Splunk Enterprise Installer package**