Top 30 Splunk Interview Questions To Prepare For In 2017

 Recommended by 50 users

[Vardhan](https://www.edureka.co/blog/author/vardhan/) Dec 9, 2016



[Add to Bookmark](https://www.edureka.co/blog/interview-questions/top-splunk-interview-questions-and-answers/)  Email this Post  4.1K [**0**](https://www.edureka.co/blog/interview-questions/top-splunk-interview-questions-and-answers/#disqus_thread)

[**Download Free Splunk E-Book**](http://resources.edureka.co/splunk-ebook/)

One thing is for certain: Implementing Splunk will transform your business and take it to the next level. But, the question is do you posses the skills to be a Splunker? If yes, then prepare yourselves for the most gruesome job interview because the competition is intense. You can start by going through the most common Splunk interview questions which are mentioned in this blog.

**Splunk Interview Questions**

<https://www.edureka.co/blog/interview-questions/top-splunk-interview-questions-and-answers/>

The questions covered in this blog post have been shortlisted after collecting inputs from many industry experts to help you ace your interview. In case you want to learn the basics of Splunk then, you can start off by reading the first blog in my Splunk tutorial series: [What Is Splunk?](http://www.edureka.co/blog/what-is-splunk/?utm_source=blog&utm_medium=content-link&utm_campaign=spunk-interview-questions) All the best!

**Q1. What is Splunk? Why is Splunk used for analyzing machine data?**

This question will most likely be the first question you will be asked in any Splunk interview. You need to start by saying that:

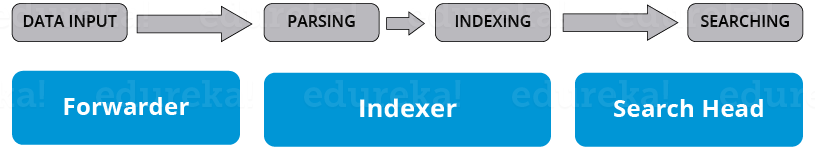
* Splunk is a platform which allows people to get visibility into machine data, that is generated from hardware devices, networks, servers, IoT devices and other sources
* Splunk is used for analyzing machine data because it can give insights into application management, IT operations, security, compliance, fraud detection, threat visibility etc

To learn more about this topic, you can read this blog: [What Is Splunk?](http://www.edureka.co/blog/what-is-splunk/?utm_source=blog&utm_medium=content-link&utm_campaign=spunk-interview-questions)

[**Read Blog**](http://www.edureka.co/blog/what-is-splunk/?utm_source=blog&utm_medium=blog-cta&utm_campaign=splunk-interview)

**Q2. Explain how Splunk works.**

This is a sure-shot question because your interviewer will judge this answer of yours to understand how well you know the concept. The Forwarder acts like a dumb agent which will collect the data from the source and forward it to the Indexer. The Indexer will store the data locally in a host machine or on cloud. The Search Head is then used for searching, analyzing, visualizing and performing various other functions on the data stored in the Indexer.



You can find more details about the working of Splunk here: [Splunk Architecture: Tutorial On Forwarder, Indexer And Search Head](http://www.edureka.co/blog/splunk-architecture/?utm_source=blog&utm_medium=content-link&utm_campaign=spunk-interview-questions" \t "_blank).

[**Read Blog**](http://www.edureka.co/blog/splunk-architecture/?utm_source=blog&utm_medium=blog-cta&utm_campaign=splunk-interview)

**Q3. What are the components of Splunk?**

Splunk Architecture is a topic which will make its way into any set of Splunk interview questions. As explained in the previous question, the main components of Splunk are **Forwarders**, **Indexers** and **Search Heads**. You can then mention that another component called **Deployment Server**(or **Management Console Host**) will come into the picture in case of a larger environment. Deployment servers:

* Act like an antivirus policy server for setting up Exceptions and Groups, so that you can map and create different set of data collection policies each for either a windows based server or a linux based server or a solaris based server
* Can be used to control different applications running in different operating systems from a central location
* Can be used to deploy the configurations and set policies for different applications from a central location.

Making use of deployment servers is an advantage because connotations, path naming conventions and machine naming conventions which are independent of every host/machine can be easily controlled using the deployment server.

**Q4. Why use only Splunk? Why can’t I go for something that is open source?**

This kind of question is asked to understand the scope of your knowledge. You can answer that question by saying that Splunk has a lot of competition in the market for analyzing machine logs, doing business intelligence, for performing IT operations and providing security. But, there is no one single tool other than Splunk that can do all of these operations and that is where Splunk comes out of the box and makes a difference. With Splunk you can easily scale up your infrastructure and get professional support from a company backing the platform. Some of its competitors are Sumo Logic in the cloud space of log management and ELK in the open source category. You can refer to the below table to understand how Splunk fares against other popular tools feature-wise. The detailed differences between these tools are covered in this blog: [Splunk vs ELK vs Sumo Logic](http://www.edureka.co/blog/splunk-vs-elk-vs-sumologic/?utm_source=blog&utm_medium=content-link&utm_campaign=spunk-interview-questions).

[**Read Blog**](http://www.edureka.co/blog/splunk-vs-elk-vs-sumologic?utm_source=blog&utm_medium=blog-cta&utm_campaign=splunk-interview)

**Q5. Which Splunk Roles can share the same machine?**

This is another frequently asked Splunk interview question which will test the candidate’s hands-on knowledge. In case of small deployments, most of the roles can be shared on the same machine which includes **Indexer**, **Search** **Head** and **License** **Master**. However, in case of larger deployments the preferred practice is to host each role on stand alone hosts. Details about roles that can be shared even in case of larger deployments are mentioned below:

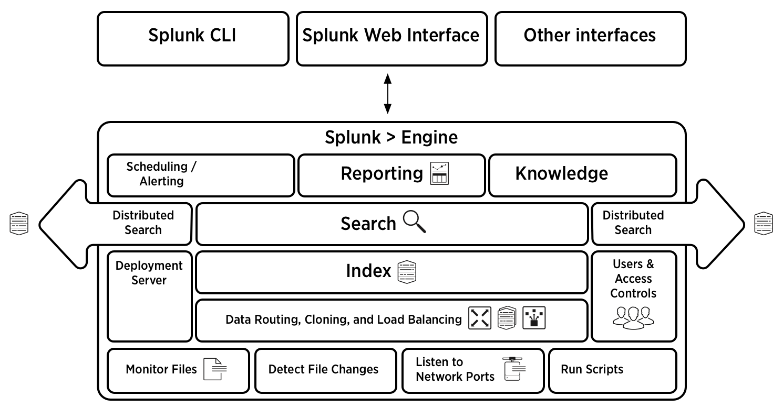
* Strategically, **Indexers** and **Search Heads** should have physically dedicated machines. Using Virtual Machines for running the instances separately is not the solution because there are certain guidelines that need to be followed for using computer resources and spinning multiple virtual machines on the same physical hardware can cause performance degradation.
* However, a **License master** and **Deployment server** can be implemented on the same virtual box, in the same instance by spinning different Virtual machines.
* You can spin another virtual machine on the same instance for hosting the **Cluster master** as long as the **Deployment master** is not hosted on a parallel virtual machine on that same instance because the number of connections coming to the **Deployment server** will be very high.
* This is because the **Deployment server** not only caters to the requests coming from the **Deployment master**, but also to the requests coming from the**Forwarders**.

**Q6. What are the unique benefits of getting data into a Splunk instance via Forwarders?**

You can say that the benefits of getting data into Splunk via forwarders are **bandwidth throttling**, **TCP connection** and an **encrypted SSL connection** for transferring data from a forwarder to an indexer. The data forwarded to the indexer is also load balanced by default and even if one indexer is down due to network outage or maintenance purpose, that data can always be routed to another indexer instance in a very short time. Also, the forwarder caches the events locally before forwarding it, thus creating a temporary backup of that data.

**Q7. Briefly explain the Splunk Architecture**

Look at the below image which gives a consolidated view of the architecture of Splunk. You can find the detailed explanation in this link: [Splunk Architecture: Tutorial On Forwarder, Indexer And Search Head](http://www.edureka.co/blog/splunk-architecture/?utm_source=blog&utm_medium=content-link&utm_campaign=spunk-interview-questions" \t "_blank).



**Q8. What is the use of License Master in Splunk?**

License master in Splunk is responsible for making sure that the right amount of data gets indexed. Splunk license is based on the data volume that comes to the platform within a 24hr window and thus, it is important to make sure that the environment stays within the limits of the purchased volume.

Consider a scenario where you get 300 GB of data on day one, 500 GB of data the next day and 1 terabyte of data some other day and then it suddenly drops to 100 GB on some other day. Then, you should ideally have a 1 terabyte/day licensing model. The license master thus makes sure that the indexers within the Splunk deployment have sufficient capacity and are licensing the right amount of data.

**Q9. What happens if the License Master is unreachable?**

In case the license master is unreachable, then it is just not possible to search the data. However, the data coming in to the Indexer will not be affected. The data will continue to flow into your Splunk deployment, the Indexers will continue to index the data as usual however, you will get a warning message on top your Search head or web UI saying that you have exceeded the indexing volume and you either need to reduce the amount of data coming in or you need to buy a higher capacity of license.

Basically, the candidate is expected to answer that the indexing does not stop; only searching is halted.

**Q10. Explain ‘license violation’ from Splunk perspective.**

If you exceed the data limit, then you will be shown a ‘license violation’ error. The license warning that is thrown up, will persist for 14 days. In a commercial license you can have 5 warnings within a 30 day rolling window before which your Indexer’s search results and reports stop triggering. In a free version however, it will show only 3 counts of warning.

**Q11. Give a few use cases of Knowledge objects.**

Knowledge objects can be used in many domains. Few examples are:

**Physical Security:** If your organization deals with physical security, then you can leverage data containing information about earthquakes, volcanoes, flooding, etc to gain valuable insights

**Application Monitoring:** By using knowledge objects, you can monitor your applications in real-time and configure alerts which will notify you when your application crashes or any downtime occurs

**Network Security:** You can increase security in your systems by blacklisting certain IPs from getting into your network. This can be done by using the Knowledge object called lookups

**Employee Management:** If you want to monitor the activity of people who are serving their notice period, then you can create a list of those people and create a rule preventing them from copying data and using them outside

**Easier Searching Of Data:** With knowledge objects, you can tag information, create event types and create search constraints right at the start and shorten them so that they are easy to remember, correlate and understand rather than writing long searches queries. Those constraints where you put your search conditions, and shorten them are called event types.

These are some of the operations that can be done from a non-technical perspective by using knowledge objects. Knowledge objects are the actual application in business, which means Splunk interview questions are incomplete without Knowledge objects. In case you want to read more about the different knowledge objects available and how they can be used, read this blog: [Splunk Tutorial On Knowledge Objects](http://www.edureka.co/blog/splunk-timechart-data-models-alert/?utm_source=blog&utm_medium=content-link&utm_campaign=splunk-interview-questions-and-answers" \t "_blank)

[**Read Blog**](http://www.edureka.co/blog/splunk-timechart-data-models-alert/?utm_source=blog&utm_medium=blog-cta&utm_campaign=splunk-interview)

**Q12. Why should we use Splunk Alert?** **What are the different options while setting up Alerts?**

This is a common question aimed at candidates appearing for the role of a Splunk Administrator. Alerts can be used when you want to be notified of an erroneous condition in your system. For example, send an email notification to the admin when there are more than three failed login attempts in a twenty-four hour period. Another example is when you want to run the same search query every day at a specific time to give a notification about the system status.

Different options that are available while setting up alerts are:

* You can create a web hook, so that you can write to hipchat or github. Here, you can write an email to a group of machines with all your subject, priorities, and body of the message
* You can add results, .csv or pdf or inline with the body of the message to make sure that the recipient understands where this alert has been fired, at what conditions and what is the action he has taken
* You can also create tickets and throttle alerts based on certain conditions like a machine name or an IP address. For example, if there is a virus outbreak, you do not want every alert to be triggered because it will lead to many tickets being created in your system which will be an overload. You can control such alerts from the alert window.

You can find more details about this topic in this blog: [Splunk alerts](http://www.edureka.co/blog/splunk-timechart-data-models-alert/?utm_source=blog&utm_medium=content-link&utm_campaign=splunk-interview-questions-and-answers" \t "_blank).

**Q13. Explain Workflow Actions**

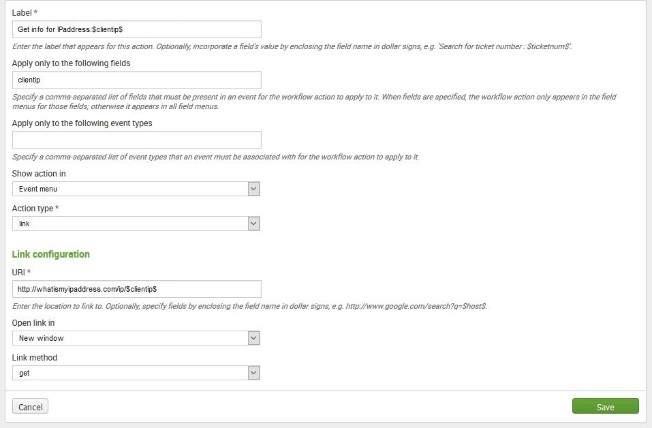
Workflow actions is one such topic that will make a presence in any set of Splunk Interview questions. Workflow actions is not common to an average Splunk user and can be answered by only those who understand it completely. So it is important that you answer this question aptly.

You can start explaining Workflow actions by first telling why it should be used.

Once you have assigned rules, created reports and schedules then what? It is not the end of the road! You can create workflow actions which will automate certain tasks. For example:

* You can do a double click, which will perform a drill down into a particular list containing user names and their IP addresses and you can perform further search into that list
* You can do a double click to retrieve a user name from a report and then pass that as a parameter to the next report
* You can use the workflow actions to retrieve some data and also send some data to other fields. A use case of that is, you can pass latitude and longitude details to google maps and then you can find where an IP address or location exists.

The screenshot below shows the window where you can set the workflow actions.



**Q14. Explain Data Models and Pivot**

Data models are used for creating a structured hierarchical model of your data. It can be used when you have a large amount of unstructured data, and when you want to make use of that information without using complex search queries.

A few use cases of Data models are:

* **Create Sales Reports:**If you have a sales report, then you can easily create the total number of successful purchases, below that you can create a child object containing the list of failed purchases and other views
* **Set Access Levels:** If you want a structured view of users and their various access levels, you can use a data model
* **Enable Authentication:** If you want structure in the authentication, you can create a model around VPN, root access, admin access, non-root admin access, authentication on various different applications to create a structure around it in a way that normalizes the way you look at data.  
  So when you look at a data model called authentication, it will not matter to Splunk what the source is, and from a user perspective it becomes extremely simple because as and when new data sources are added or when old one’s are deprecated, you do not have to rewrite all your searches and that is the biggest benefit of using data models and pivots.

On the other hand with pivots, you have the flexibility to create the front views of your results and then pick and choose the most appropriate filter for a better view of results. Both these options are useful for managers from a non-technical or semi-technical background. You can find more details about this topic in this blog: [Splunk Data Models](http://www.edureka.co/blog/splunk-timechart-data-models-alert/?utm_source=blog&utm_medium=content-link&utm_campaign=splunk-interview-questions-and-answers" \t "_blank).

[**Check Out Splunk Course**](http://www.edureka.co/splunk/?utm_source=blog&utm_medium=blog-cta&utm_campaign=splunk-interview)

**Q15. Explain Search Factor (SF) & Replication Factor (RF)**

Questions regarding Search Factor and Replication Factor are most likely asked when you are interviewing for the role of a Splunk Architect. SF & RF are terminologies related to Clustering techniques (Search head clustering & Indexer clustering).

* The search factor determines the number of searchable copies of data maintained by the indexer cluster. The default value of search factor is 2. However, the Replication Factor in case of Indexer cluster, is the number of copies of data the cluster maintains and in case of a search head cluster, it is the minimum number of copies of each search artifact, the cluster maintains
* Search head cluster has only a Search Factor whereas an Indexer cluster has both a Search Factor and a Replication Factor
* Important point to note is that the search factor must be less than or equal to the replication factor

**Q16. Which commands are included in ‘filtering results’ category?**

There will be a great deal of events coming to Splunk in a short time. Thus it is a little complicated task to search and filter data. But, thankfully there are commands like ‘search’, ‘where’, ‘sort’ and ‘rex’ that come to the rescue. That is why, filtering commands are also among the most commonly asked Splunk interview questions.

**Search**: The ‘search’ command is used to retrieve events from indexes or filter the results of a previous search command in the pipeline. You can retrieve events from your indexes using keywords, quoted phrases, wildcards, and key/value expressions. The ‘search’ command is implied at the beginning of any and every search operation.

**Where**: The ‘where’ command however uses ‘eval’ expressions to filter search results. While the ‘search’ command keeps only the results for which the evaluation was successful, the ‘where’ command is used to drill down further into those search results. For example, a ‘search’ can be used to find the total number of nodes that are active but it is the ‘where’ command which will return a matching condition of an active node which is running a particular application.

**Sort**: The ‘sort’ command is used to sort the results by specified fields. It can sort the results in a reverse order, ascending or descending order. Apart from that, the sort command also has the capability to limit the results while sorting. For example, you can execute commands which will return only the top 5 revenue generating products in your business.

**Rex**: The ‘rex’ command basically allows you to extract data or particular fields from your events. For example if you want to identify certain fields in an email id: *abc@edureka.co*, the ‘rex’ command allows you to break down the results as *abc*being the user id, *edureka.co* being the domain name and *edureka*as the company name. You can use rex to breakdown, slice your events and parts of each of your event record the way you want.

**Q17. What is a *lookup*command? Differentiate between *inputlookup* & *outputlookup* commands.**

Lookup command is that topic into which most interview questions dive into, with questions like: Can you enrich the data? How do you enrich the raw data with external lookup?   
You will be given a use case scenario, where you have a csv file and you are asked to do lookups for certain product catalogs and asked to compare the raw data & structured csv or json data. So you should be prepared to answer such questions confidently.

**Lookup commands** are used when you want to receive some fields from an external file (such as CSV file or any python based script) to get some value of an event. It is used to narrow the search results as it helps to reference fields in an external CSV file that match fields in your event data.

An ***inputlookup***basically takes an input as the name suggests. For example, it would take the product price, product name as input and then match it with an internal field like a product id or an item id. Whereas, an ***outputlookup***is used to generate an output from an existing field list. Basically, inputlookup is used to enrich the data and outputlookup is used to build their information.

[**View Course Curriculum**](http://www.edureka.co/splunk/?utm_source=blog&utm_medium=blog-cta&utm_campaign=splunk-interview)

**Q18. What is the difference between ‘eval’, ‘stats’, ‘charts’ and ‘timecharts’ command?**

‘Eval’ and ‘stats*’*are among the most common as well as the most important commands within the Splunk SPL language and they are used interchangeably in the same way as ‘search’ and ‘where’ commands.

* At times ‘eval’ and ‘stats’ are used interchangeably however, there is a subtle difference between the two. While ‘stats*‘*command is used for computing statistics on a set of events, ‘eval’ command allows you to create a new field altogether and then use that field in subsequent parts for searching the data.
* Another frequently asked question is the difference between ‘stats’, ‘charts’ and ‘timecharts’ commands. The difference between them is mentioned in the table below.

|  |  |  |
| --- | --- | --- |
| **Stats** | **Chart** | **Timechart** |
| Stats is a reporting command which is used to present data in a tabular format. | Chart displays the data in the form of a bar, line or area graph. It also gives the capability of generating a pie chart. | Timechart allows you to look at bar and line graphs. However, pie charts are not possible. |
| In Stats command, you can use multiple fields to build a table. | In Chart, it takes only 2 fields, each field on X and Y axis respectively. | In Timechart, it takes only 1 field since the X-axis is fixed as the time field. |

**Q19. What are the different types of Data Inputs in Splunk?**

This is the kind of question which only somebody who has worked as a Splunk administrator can answer. The answer to the question is below.

* The obvious and the easiest way would be by using files and directories as input
* Configuring Network ports to receive inputs automatically and writing scripts such that the output of these scripts is pushed into Splunk is another common way
* But a seasoned Splunk administrator, would be expected to add another option called windows inputs. These windows inputs are of 4 types: registry inputs monitor, printer monitor, network monitor and active directory monitor.

**Q20. What are the defaults fields for every event in Splunk?**

There are about 5 fields that are default and they are barcoded with every event into Splunk.  
They are host, source, source type, index and timestamp.

**Q21. Explain file precedence in Splunk.**

File precedence is an important aspect of troubleshooting in Splunk for an administrator, developer, as well as an architect. All of Splunk’s configurations are written within plain text .conf files. There can be multiple copies present for each of these files, and thus it is important to know the role these files play when a Splunk instance is running or restarted. File precedence is an important concept to understand for a number of reasons:

* To be able to plan Splunk upgrades
* To be able to plan app upgrades
* To be able to provide different data inputs and
* To distribute the configurations to your splunk deployments.

To determine the priority among copies of a configuration file, Splunk software first determines the directory scheme. The directory schemes are either a) Global or b) App/user.

When the context is global (that is, where there’s no app/user context), directory priority descends in this order:

1. System local directory — *highest priority*
2. App local directories
3. App default directories
4. System default directory — *lowest priority*

When the context is app/user, directory priority descends from user to app to system:

1. User directories for current user — *highest priority*
2. App directories for currently running app (local, followed by default)
3. App directories for all other apps (local, followed by default) — for exported settings only
4. System directories (local, followed by default) — *lowest priority*

**Q22. How can we extract fields?**

You can extract fields from either event lists, sidebar or from the settings menu via the UI.  
The other way is to write your own regular expressions in props.conf configuration file.

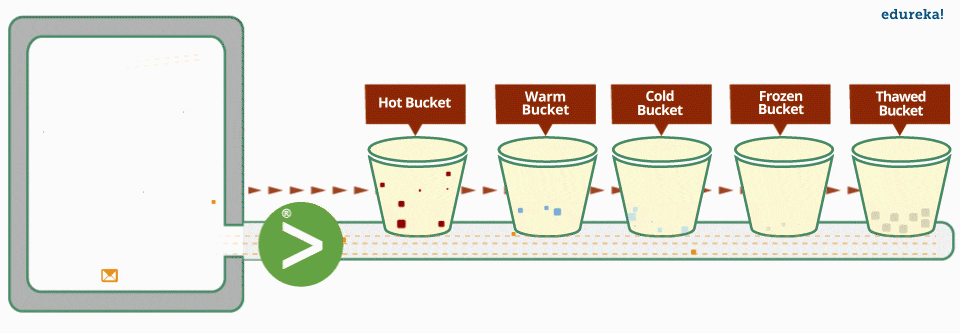
**Q23. What is the difference between Search time and Index time field extractions?**

As the name suggests, Search time field extraction refers to the fields extracted while performing searches whereas, fields extracted when the data comes to the indexer are referred to as Index time field extraction. You can set up the indexer time field extraction either at the forwarder level or at the indexer level.

Another difference is that Search time field extraction’s extracted fields are not part of the metadata, so they do not consume disk space. Whereas index time field extraction’s extracted fields are a part of metadata and hence consume disk space.

**Q24. Explain how data ages in Splunk?**

Data coming in to the indexer is stored in directories called buckets. A bucket moves through several stages as data ages: **hot**, **warm**, **cold**, **frozen** and**thawed**. Over time, buckets ‘roll’ from one stage to the next stage.



* The first time when data gets indexed, it goes into a **hot bucket**. Hot buckets are both searchable and are actively being written to. An index can have several hot buckets open at a time
* When certain conditions occur (for example, the hot bucket reaches a certain size or *splunkd*gets restarted), the hot bucket becomes a **warm bucket**(“rolls to warm”), and a new hot bucket is created in its place. Warm buckets are searchable, but are not actively written to. There can be many warm buckets
* Once further conditions are met (for example, the index reaches some maximum number of warm buckets), the indexer begins to roll the warm buckets to**cold** based on their age. It always selects the oldest warm bucket to roll to cold. Buckets continue to roll to cold as they age in this manner
* After a set period of time, cold buckets roll to **frozen**, at which point they are either archived or deleted.

The bucket aging policy, which determines when a bucket moves from one stage to the next, can be modified by editing the attributes in indexes.conf.

[**Get Started with Splunk**](http://www.edureka.co/splunk/?utm_source=blog&utm_medium=blog-cta&utm_campaign=splunk-interview)

**Q25. What is summary index in Splunk?**

Summary index is another important Splunk interview question from an administrative perspective. You will be asked this question to find out if you know how to store your analytical data, reports and summaries. The answer to this question is below.

The **biggest advantage** of having a summary index is that you can retain the analytics and reports even after your data has aged out. For example:

* Assume that your data retention policy is only for 6 months but, your data has aged out and is older than a few months. If you still want to do your own calculation or dig out some statistical value, then during that time, summary index is useful
* For example, you can store the summary and statistics of the percentage growth of sale that took place in each of the last 6 months and you can pull the average revenue from that. That average value is stored inside summary index.

But the **limitations** with summary index are:

* You cannot do a needle in the haystack kind of a search
* You cannot drill down and find out which products contributed to the revenue
* You cannot find out the top product from your statistics
* You cannot drill down and nail which was the maximum contribution to that summary.

That is the use of Summary indexing and in an interview, you are expected to answer both these aspects of benefit and limitation.

**Q26. How to exclude some events from being indexed by Splunk?**

You might not want to index all your events in Splunk instance. In that case, how will you exclude the entry of events to Splunk.  
An example of this is the debug messages in your application development cycle. You can exclude such debug messages by putting those events in the null queue. These null queues are put into **transforms.conf** at the forwarder level itself.

If a candidate can answer this question, then he is most likely to get hired.

**Q27. What is the use of Time Zone property in Splunk? When is it required the most?**

Time zone is extremely important when you are searching for events from a security or fraud perspective. If you search your events with the wrong time zone then you will end up not being able to find that particular event altogether. Splunk picks up the default time zone from your browser settings. The browser in turn picks up the current time zone from the machine you are using. Splunk picks up that timezone when the data is input, and it is required the most when you are searching and correlating data coming from different sources. For example, you can search for events that came in at 4:00 PM IST, in your London data center or Singapore data center and so on. The timezone property is thus very important to correlate such events.

**Q28. What is Splunk App? What is the difference between Splunk App and Add-on?**

Splunk Apps are considered to be the entire collection of reports, dashboards, alerts, field extractions and lookups.   
Splunk Apps minus the visual components of a report or a dashboard are Splunk Add-ons. Lookups, field extractions, etc are examples of Splunk Add-on.

Any candidate knowing this answer will be the one questioned more about the developer aspects of Splunk.

**Q29. How to assign colors in a chart based on field names in Splunk UI?**

You need to assign colors to charts while creating reports and presenting results. Most of the time the colors are picked by default. But what if you want to assign your own colors? For example, if your sales numbers fall below a threshold, then you might need that chart to display the graph in red color. Then, how will you be able to change the color in a Splunk Web UI?

You will have to first edit the panels built on top of a dashboard and then modify the panel settings from the UI. You can then pick and choose the colors. You can also write commands to choose the colors from a palette by inputting hexadecimal values or by writing code. But, Splunk UI is the preferred way because you have the flexibility to assign colors easily to different values based on their types in the bar chart or line chart. You can also give different gradients and set your values into a radial gauge or water gauge.

**Q30. What is sourcetype in Splunk?**

Now this question may feature at the bottom of the list, but that doesn’t mean it is the least important among other Splunk interview questions.

Sourcetype is a default field which is used to identify the data structure of an incoming event. Sourcetype determines how Splunk Enterprise formats the data during the indexing process. Source type can be set at the forwarder level for indexer extraction to identify different data formats. Because the source type controls how Splunk software formats incoming data, it is important that you assign the correct source type to your data. It is important that even the indexed version of the data (the event data) also looks the way you want, with appropriate timestamps and event breaks. This facilitates easier searching of data later.

For example, the data maybe coming in the form of a csv, such that the first line is a header, the second line is a blank line and then from the next line comes the actual data. Another example where you need to use sourcetype is if you want to break down date field into 3 different columns of a csv, each for day, month, year and then index it. Your answer to this question will be a decisive factor in you getting recruited.

[**Learn Splunk From Experts**](http://www.edureka.co/splunk/?utm_source=blog&utm_medium=blog-cta&utm_campaign=splunk-interview)

I hope this set of Splunk interview questions will help you in preparing for your interview. You can check out the different job roles, a Splunk skilled professional is liable for by reading this blog on [Splunk Careers](http://www.edureka.co/blog/splunk-careers-big-data-jobs?utm_source=blog&utm_medium=content-link&utm_campaign=spunk-interview-questions" \t "_blank). Also, we have the video on Splunk Interview Questions by an expert which can help you further. Do take a look and let us know if this helped in your interview preparation.

**Top Splunk Interview Questions and Answers | Splunk Careers & Jobs | Splunk Tutorial | Edureka**