By OnlineInterviewQuestions.com

Splunk Interview Questions and Answers

Splunk is a software technology that is the first data-to-everything platform. It is mainly used for monitoring, searching, analyzing, and visualizing machine-generated data in real-time. It was founded in October 2003 (About 17 years ago) by Michael Baum, Rob Das, & Erik Swan. It is headquartered in San Francisco, California, U.S.

We have listed below the **25+ best Splunk Interview Questions and Answers**. these **Splunk Interview Questions** are very helpful for the preparation of the Splunk Interview. You can also download here the **Splunk Interview Questions PDF**.

Q1. What is splunk tool?

Splunk is a leading tool for log management. It is widely used for monitoring, searching, analyzing and visualizing the machine-generated data in real time.

Q2. What is Splunk?

Splunk is a software technology which is the first data to everything platform. It is mainly used for **monitoring**, **searching**, **analyzing**, and **visualizing the machine-generated data in the real-time**. It is the best-suited tool for the root cause analysis. It has an enhanced GUI that allows you to create graphs, alerts. With this, you can troubleshoot any condition failure for improved performance.

Splunk products are available in three different versions. They are

1. Splunk Enterprise,
2. Splunk Light, and
3. Splunk Cloud.

Q3. Enlist major components of Splunk?

The three main components in Splunk are

1. Splunk Forwarder,
2. Splunk Indexer, and
3. Splunk Head.

Splunk Forwarder - This component is used for collecting logs. They are independent of the main Splunk instance and are used to collect logs from the remote machine. After collecting the logs, the Splunk Forwarder will forward the log data to a Splunk Indexer for processing and storage.

Splunk Indexer - It is used for indexing and storing the data from the Splunk forwarder. As it indexes the data, the Splunk Indexer creates a number of files. These files contain any one of either item like the raw data in compressed form or the indexes that point to raw data.

Splunk Search Head - This component is used for interacting with the Splunk. It provides GUI for the user to do various operations with the Splunk.

Q4. What is Splunk Indexer?

The Indexer is one of the components present in the Splunk which is used for **indexing** and **storing the data coming from the forwarder**. It transforms the incoming data into events and stores the event in the indexes for efficiently performing the search operations. If the data is received from a universal forwarder, then the indexer will parse the incoming data and index it. If the data is received from the heavy forwarder, then indexer will only index the data. The Splunk Indexer creates number of files as it indexes the data that may contain either the compressed raw data or the indexes that point to the raw data.

Q5. List different types of Splunk Licenses?

Several types of Splunk licenses include,

- **The Splunk Enterprise license -** it includes all the enterprise features such as authentication and distributed search. Several types of Splunk Enterprise license include the Splunk Enterprise Trial license, and Splunk for Industrial IoT license.
- **The Free license -** Some features are disabled in this free license like the authentication feature. It allows for a limited indexing volume.
- **The Forwarder license -** it is used with the forwarders as it allows only to forward and not index the data.
- **The Beta license -** it has enterprise features but is restricted to Splunk software Beta releases.

Q6. What is the Summary Index in Splunk?

Summary Index is used for storing historical time series data for **statistical analysis**, **anomaly detection**, and **machine learning efforts**. A summary index is a Splunk index that stores the results of a report that is scheduled. It enables you to run fast searches over large data sets by spreading the cost of a computationally expensive report over time. The Summary Index can be created like other Splunk Indexes.

Q7. What is Splunk DB Connect?

The Splunk DB connect is used to **import tables**, **rows**, and **columns** from a database to the Splunk Enterprise directly. This is used to combine the structured data from the databases with unstructured machine data. After this, Splunk Enterprise is used to provide insights into all the combined data. With DB connect, you can also enable the output data from the Splunk Enterprise back to your relational database. You can also perform database lookups using the Splunk DB Connect.

Q8. How to start or stop the Splunk server?

The command **NET START <service>** or **NET STOP <service>** is used to start or stop a Splunk Enterprise process. These commands are executed in the Windows services control panel and are exclusive to Windows. In the Unix systems, you can run the **"#splunk start"** or **"#splunk restart"** in the command shell to start or restart the Splunk server.

Q9. How to disable Splunk boot-start?

You can run the **"disable boot-start"** command to remove the Splunk init script located at the **/etc/init.d**

Q10. What is Fishbucket in Splunk?

Fishbucket in Splunk is a sub-directory that is used to **monitor** or **track** internally how far the content of your file is indexed in the Splunk. It has two contents to achieve this feature such as **seek pointers** and **CRC** (**Cyclic Redundancy Check**). The default location of the fish bucket sub-directory is the **$splunk_home/splunk/var/lib**.

Q11. List operating system supported by Splunk?

The operating systems supported by the Splunk are,

- Linux, 2.6 and later
- Linux, all 3.x and 4.x kernel versions
- Mac OS X 10.13 and 10.14
- Mac OS X 10.12
- Windows Server 2016
- Windows Server 2012, Server 2012 R2
- Windows 10 (64 bit, and 32 bit)
- Windows 8.1 (64 bit, and 32 bit)

Q12. For what Splunk is mainly used?

Splunk is used for **searching**, **monitoring**, and **examining** the machine-generated data. It does this using a web-style interface. It also performs capturing, indexing, and correlating the real-time data. It does this in the searchable container. From this, the Splunk can produce graphs, reports, alerts, dashboards, and visualizations. Splunk technology is mainly used for application management, security, and compliance. Splunk helps to access the machine-generated data that will be useful for everyone.

Q13. What is Splunk enterprise?

Splunk Enterprise enables you to **search**, **analyze**, and **visualize the data**. It helps to do this by gathering the data from the components of the **IT infrastructure** or **business**. It indexes the data stream and parses it into a series of individual events for you to view and search. Splunk Enterprise has various features such as indexing the data, searching the data to retrieve an event, notifying when search result meets the configured conditions, and more. It also provides dashboards that contains panels of search boxes, fields, charts, and more.

Q14. What are Splunk logs?

The log files in Splunk are located at **$SPLUNK_HOME/var/log/splunk** for the internal log, and **$SPLUNK_HOME/var/log/introspection** for the introspection logs. The log records contain data about the impact of the Splunk software on the host system. There is also a Splunk search log that is located at the **$SPLUNK_HOME/var/run/splunk/dispatch/**. The search log contains the data about the search operation including the run time and other performance metrics.

Q15. How Splunk differs from AppDynamics?

The AppDynamics and Splunk are both used for **APM practice**. But they differ in some ways.

AppDynamics is a popular application monitoring system in the world. It can automatically map application business transaction to see the performance issued from an overhead perspective. It has support for **Java**, **.net**, **PHP**, **Node JS**, **C++**, **Python**, and **Go**. Companies like **Vodafone**, **Nasdaq**, **Dixons Carphone**, **eHarmony**, and the **World Bank** are some of the popular clients of AppDynamics.

Splunk allows you to monitor the connected applications via the use of machine data. You can view the resource usage of the app in real-time. It also converts the log data into metrics. Companies like **Coca-Cola**, **CloudShare**, **Domino's**, **John Lewis**, and **Tesco** are some of the popular clients of the Splunk.

Q16. What is Splunk light?

Splunk Light is a **comprehensive Splunk package**. This comprehensive package is used by small IT environments. It performs log search and analysis. It also provides monitoring and troubleshooting solutions for **analysts**

, **administrators**, and **developers**.

Some Features of the Splunk light are event indexing, metrics indexing, freeform search, monitoring, alerting, report analysis, add-ons, and custom dashboards.

Q17. What is source type in Splunk?

The source type is the default fields that are assigned to the incoming data by the Splunk software. It controls how the Splunk software formats the incoming data so you can categorize the data for easy searching. There are a lot of pre-defined source types available in Splunk which the Splunk software automatically selects based on the incoming data. But if the data is specialized, then you should create a new source type. You can use the source type field to search for event data after it is indexed.

Some of the common source types are,

- Access_combines
- Apache_error
- Cisco_syslog
- websphere_core

Q18. List some Splunk basic commands?

Some of the basic Splunk commands are,

- **Abstract -** it produces a summary for each search results
- **Accum -** it keeps a running total of a specified numeric field
- **Bucketdir -** It replaces a field value with higher-level grouping
- **Chart -** it is used to return results in a tabular output for charting
- **Cluster -** it is used to cluster similar events together
- **Delta -** it is used to compute the difference between two search results
- **Eval -** it calculates the expression and puts the result into a field
- **Guage -** it transforms the result into a format suitable for display by the gauge chart types
- **K-means -** it performs k-means clustering on selecting fields
- **Search -** it searches the Splunk indexed for matching events
- **Sort -** it sorts the search results by the specified fields
- **Top -** it is used to display the most common values of a field

Q19. What are the important configuration files of Splunk?

Some of the important configuration files in the Splunk are,

1. **App.conf -** it is used to configure the app properties
2. **Authorize.conf -** it is used to configures roles

3. **Bookmarks.conf -** it is used to bookmark the monitoring console URLs
4. **Collections.conf -** it is used to configure the KV Store collections for apps
5. **Eventtypes.conf -** it is used to create event type definitions
6. **Indexes.conf -** it is used to manage and configure index settings
7. **Inputs.conf -** it is used to set up the data inputs
8. **Searchbnf.conf -** it is used to configure the search assistant
9. **Web.conf -** it is used to configure the Splunk Web

Q20. What are Splunk buckets?

Buckets in the Splunk are used to store the indexed data. Buckets are the directories that contain both the data and index files into the data. The index cluster replicates the data on the bucket-by-bucket basis. The original bucket copy and the replicated copies present on the peer nodes contain the identical sets of data.

Q21. What is KV store in Splunk?

The KV store is used to store the data as **key-value pairs**. It stores the key-value pairs as a collection. Important concepts in the KV store are the **collections**, **Records**, **Fields**, **_key**, **_user**. To add a KV store functionality to your app, you need to create a collection and define a list of fields with data types. Then, perform create-read-update-delete operations. Finally, manage the collections using the REST API.

Q22. What Lookup commands do in Splunk?

The lookup command is used to **invoke field value lookups**. The required arguments in the lookup commands are the lookup table name, the local bool value, update bool value, lookup field, event field, and event destfield. If the output or outputnew clause is not specified in the lookup command, then all the fields that are not a match are used as output fields.

Q23. What are alerts in Splunk?

The alerts in Splunk are actions. It gets triggered when a specific criterion is met. The criterion is specified by the user. It can be used to perform different actions like **logging an action**, **send an email**, or **output a result** to the lookup file.

Q24. What is Splunk forwarder?

The Splunk forwarder is a free, dedicated version of Splunk Enterprise. It contains only the essential components used to forward data. It is designed to run on a production server that has a **minimal CPU** and **memory usage** so it has the least impact possible on **mission-critical** software.

Q25. What is deployer in Splunk?

The deployer in Splunk is used to **distribute apps** and other **configuration updates** to search head cluster members. It is used to distribute the configuration bundle in response to your command. It also distributes the bundle when a member joins or rejoins the cluster. The three main roles of the deployer are,

- It is used to handle the migration of app and user configuration.
- It deploys the baseline app configurations to search head cluster members.
- It distributes the non-replicated, non-runtime configuration updates. It distributes the updates to all search head cluster members.

Q26. What is btool in Splunk?

The Btool in Splunk is a command-line tool. It is used to **troubleshoot** and help with your **configuration files**. It is also used to see what values are used by the Splunk instance.

Q27. How to change the default port in Splunk?

To change the port, you can use **Splunk CLI**. Use the set command to change the port.

```
//example splunk set web-port 9000
```

The above command sets the port to 9000.