**os commands for shell scripting:**

**1.ls (list)**

**2.pwd (present working directory)**

**3.cd (change directory) (file in)**

**4.cd .. (file out)**

**5.mkdir (main directory)**

**6.vim (create file)**

**7.touch file nme.txt (create file)**

**8.mv (move file)**

**9.clear**

**10.echo(print of the data)**

https://www.youtube.com/watch?v=U2J8KRemwMo

**\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\***

**python group by practice:**

<https://www.youtube.com/watch?v=R6fyzDIOOH4>

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

**splunk tools basic understanding:**

https://www.youtube.com/watch?v=ru4EJxOignE

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

**POSTMAN GET METHOD**:

1.This is an HTTP request which is sent to the server when something is to be retrieved from the server.

2.Get request is safe as it does not change anything on the server.

3. When the same Get request is sent to the server, the same result is expected.

4.A GET request has all its information inside the URL,

5. URL is visible all the time, it is advisable not to use this type of request while you send some sensitive information such as passwords.

6.A GET request is used to get the information from the server and does not have any side effects on the server. Side-effects mean there is no updation/deletion/addition of data on the server

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

**Amazon QuickSight:**

Amazon QuickSight is a unified business intelligence service that makes it easier for all employees within an organization to build visualizations, perform ad hoc analysis, and quickly get business insights from their data, anytime, on any device.

Quicksight provides easy to use tools to build visualizations, perform ad-hoc analysis, get business insights from the data and share the results with others.

Amazon QuickSight is a cloud-scale business intelligence (BI) service that you can use to deliver easy-to-understand insights to the people who you work with, wherever they are. Amazon QuickSight connects to your data in the cloud and combines data from many different sources.

one or more programming languages, such as JavaScript, Java, Python, or C#.

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

**Here are the main Splunk search types:**

1. Simple Search

- Keyword search

- Phrase search

- Field-value search

- Wildcard search

Example: error, "error message", status=404, error\*

2. Advanced Search

- Boolean search (AND, OR, NOT)

- Grouping (parentheses)

- Regular expression (regex) search

Example: (error OR warning) AND status=404, regex error\d+

3. Statistical Search

- Statistical functions (e.g., sum, avg, count)

- Chart search

- Timechart search

Example: stats count by status, chart sum(bytes) over time

4. Data Analysis Search

- Pivot search

- Data model search

- Lookup search

- Correlation search

Example: pivot table sum(bytes) by source, datamodel Network\_Traffic

5. Transactional Search

- Transaction search

- Event grouping

Example: transaction id=123, eventgroup transaction\_id=456

6. Geographic Search

- Geographic location search

- IP address search

Example: geoip country="USA", ip\_address="192.168.1.1"

7. Time-Based Search

- Time range search

- Date search

Example: \_time>=-1h, \_time>=2022-01-01

8. Subsearch

- Search within search results

Example: [search error]

9. Saved Search

- Run saved searches

Example: savedsearch="error logs"

10. Real-Time Search

- Search in real-time

Example: realtime error

11. Historical Search

- Search historical data

Example: historical error

12. Search with Macros

- Use predefined macros

Example: error\_logs

13. Search with Lookups

- Use lookup tables

Example: lookup cities city OUTPUT population

14. Search with Data Models

- Use data models

Example: datamodel Network\_Traffic

These search types can be combined to create complex searches.

Best Practices:

1. Use meaningful search names and descriptions.

2. Optimize searches for performance.

3. Use field-value pairs for efficient searching.

4. Test searches thoroughly.

5. Document searches for future reference.

**There are several ways to search for logs in Splunk:**

1. Simple Search

- Use keywords, phrases, or field-value pairs

- Example: error, 404, status=404

2. Advanced Search

- Use Boolean operators (AND, OR, NOT)

- Use parentheses for grouping

- Example: (error OR warning) AND status=404

3. Field-Value Search

- Use field=value syntax

- Example: status=404, error\_message="connection refused"

4. Wildcard Search

- Use \* for wildcard matching

- Example: error\*, 404\*

5. Regular Expression (regex) Search

- Use regex command

- Example: regex error\d+

6. Time-Based Search

- Use \_time field

- Example: \_time>=-1h, \_time>=2022-01-01

7. Geographic Search

- Use geoip command

- Example: geoip country="USA"

8. Transactional Search

- Use transaction command

- Example: transaction id=123

9. Subsearch

- Use [subsearch] syntax

- Example: [search error]

10. Splunk Query Language (SPL)

- Use SPL commands (e.g., stats, chart, timechart)

- Example: index=\_internal | stats count by source

11. Search Templates

- Use pre-defined search templates

- Example: splunk search template="error logs"

12. Macros

- Use predefined macros

- Example: error\_logs

13. Saved Searches

- Use saved searches as a starting point

- Example: savedsearch="error logs"

14. Dashboard Searches

- Use searches within dashboards

- Example: dashboard search="error logs"

15. API Searches

- Use Splunk API to perform searches

- Example: `curl -X GET '(link unavailable)

These are just some of the ways to search for logs in Splunk. The specific search method used will depend on the use case and requirements.

Best Practices:

1. Use meaningful search names and descriptions.

2. Optimize searches for performance.

3. Use field-value pairs for efficient searching.

4. Test searches thoroughly.

5. Document searches for future reference.

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

**Log Analysis:**

Log analysis in Splunk involves examining and interpreting log data to gain insights into system performance, security, and operational issues.

Log Analysis Steps in Splunk:

1. Data Collection: Collect log data from various sources.

2. Data Indexing: Index log data for efficient searching.

3. Search and Filter: Search and filter log data using Splunk Search Processing Language (SPL).

4. Analysis: Analyze log data to identify trends, patterns, and anomalies.

5. Visualization: Visualize log data using charts, tables, and dashboards.

6. Alerting: Set up alerts for critical issues.

Log Analysis Techniques in Splunk:

1. Pattern Matching: Identify patterns in log data.

2. Anomaly Detection: Detect unusual patterns or outliers.

3. Trend Analysis: Analyze log data trends.

4. Correlation Analysis: Correlate log data with other data sources.

5. Root Cause Analysis: Identify root causes of issues.

Splunk Log Analysis Tools:

1. Splunk Search & Reporting: Search and analyze log data.

2. Splunk Dashboards: Visualize log data.

3. Splunk Alerts: Set up alerts for critical issues.

4. Splunk Reports: Generate reports on log data.

5. Splunk Analytics: Perform advanced analytics.

Log Analysis Use Cases:

1. Security Monitoring: Monitor security-related log data.

2. Compliance Monitoring: Monitor compliance-related log data.

3. IT Operations Monitoring: Monitor IT operations-related log data.

4. Application Performance Monitoring: Monitor application performance.

5. Network Monitoring: Monitor network-related log data.

Best Practices for Log Analysis in Splunk:

1. Standardize log formats.

2. Use meaningful field names.

3. Optimize search queries.

4. Use data models.

5. Monitor data quality.

Common Log Analysis Challenges:

1. Data volume and complexity.

2. Data quality issues.

3. Lack of standardization.

4. Insufficient resources.

5. Difficulty in identifying root causes.

Log Analysis Benefits:

1. Improved security.

2. Enhanced operational efficiency.

3. Better decision-making.

4. Reduced downtime.

5. Improved compliance.

By following these steps, techniques, and best practices, you can effectively analyze logs in Splunk and gain valuable insights into your system performance, security, and operational issues.