Sure! As an SRE using Splunk, you'll frequently rely on search commands to monitor application health, troubleshoot incidents, and analyze logs efficiently. Here's a list of the most useful Splunk search commands for your role:

Basic Search Commands

1. **index**= – Specifies the index to search within.

```
index=your_index
```

2. **source**= & sourcetype= – Filters results based on log source or type.

```
index=your_index source="/var/log/app.log"
```

3. host= – Filters logs from a specific server.

```
index=your_index host=your_server
```

Filtering and Field Extraction

4. fields – Selects specific fields to display.

```
index=your_index | fields _time, host, message
```

5. where – Applies a condition filter.

```
index=your_index | where response_time > 500
```

6. rex – Extracts values using regex.

```
index=your_index | rex "User: (?<username>\w+)"
```

Statistical and Aggregation Commands

7. stats – Computes aggregates like count, avg, sum, etc.

```
index=your_index | stats count by host
```

8. timechart – Creates a time-based chart.

```
index=your_index | timechart avg(response_time) by host
```

9. tstats – Optimized for large datasets.

```
| tstats count where index=your_index by _time span=1h
```

Performance Monitoring & Troubleshooting

10. top & rare – Finds most/least common values.

```
index=your_index | top error_code
```

11. transaction – Groups related events.

```
index=your_index | transaction user_id maxspan=30s
```

12. eval – Creates new fields with calculations.

```
index=your_index | eval response_ms=response_time*1000
```

Alerting & Incident Handling

13. eventstats – Computes stats across events.

```
index=your_index | eventstats avg(response_time) as avg_time by host
```

14. lookup – Enriches logs with external data.

```
index=your_index | lookup user_details.csv user_id OUTPUT name, department
```

15. dedup – Removes duplicate results.

```
index=your_index | dedup user_id
```

Log Analysis & Pattern Matching

16. regex – Filters based on regex pattern.

```
index=your_index | regex _raw="error|fail|timeout"
```

17. bin – Groups values into bins (useful for histograms).

```
index=your_index | bin duration span=10
```

18. spath – Extracts JSON/XML fields.

```
index=your_index | spath input=_raw path=event.details
```

Incident Response & RCA

19. append – Combines multiple searches.

```
search1 | append [search search2]
```

20. join – Joins data from different sources.

```
index=your_index | join user_id [search index=another_index]
```