Splunk Admin Interview Questions (L1–L3)

L1 Questions:

1. What is Splunk?

2. What are the main components of Splunk?

3. Difference between UF and HF?

4. What is a Sourcetype?

5. What is an Index?

6. How do you check Splunk service status?

7. Common Splunk ports?

8. How do you check forwarder connectivity?

L2 Questions:

9. What is props.conf?

10. What is transforms.conf?

11. Difference between Search Time and Index Time extraction?

12. Purpose of Deployment Server?

13. Explain Indexer Clustering.

14. Explain Search Head Clustering.

15. How do you troubleshoot missing logs?

L3 Questions:

16. What are Splunk Buckets?

17. What is tstats?

18. What is Summary Indexing?

19. How do you optimize Splunk searches?

20. What to do in case of Indexer Cluster Peer Failure?

This PDF contains a compact, interview-ready Splunk Admin Q&A; list.