Troubleshooting Splunk Q&A (Modules 1-7)

1. Q: How can you improve search performance for users?

A: By using base searches, search macros, event sampling, and indexing best practices.

2. Q: How can duplicate indexing be detected?

A: By checking splunkd logs for WatchedFile component and comparing _indextime values.

3. Q: What component helps distribute search loads across peers?

A: The Search Head and Search Peer topology.

4. Q: What are signs that apps are not deploying properly to clients?

A: Clients may not contact the correct DS, or whitelist/blacklist settings might be incorrect.

5. Q: How can you detect skipped or delayed searches?

A: By checking scheduler.log and looking for 'skipped' entries.

6. Q: What does a 'blocked=true' status in a queue indicate?

A: That the queue is full and processing is delayed or halted.

7. Q: How can you improve search performance for users?

A: By using base searches, search macros, event sampling, and indexing best practices.

8. Q: What component helps distribute search loads across peers?

A: The Search Head and Search Peer topology.

9. Q: How can you improve search performance for users?

A: By using base searches, search macros, event sampling, and indexing best practices.

10. Q: How can duplicate indexing be detected?

A: By checking splunkd logs for WatchedFile component and comparing _indextime values.

11. Q: Where do you find errors related to search artifacts or permissions?

A: In the splunkd.log or audit.log.

12. Q: What are signs that apps are not deploying properly to clients?

A: Clients may not contact the correct DS, or whitelist/blacklist settings might be incorrect.

13. Q: What are signs that apps are not deploying properly to clients?

A: Clients may not contact the correct DS, or whitelist/blacklist settings might be incorrect.

14. Q: What is the fishbucket and its role?

A: It stores CRC and seek pointers to prevent re-indexing files.

15. Q: Which component determines the event boundary and performs timestamp extraction?

A: The aggregator processor in the merging pipeline.

16. Q: How can you improve search performance for users?

A: By using base searches, search macros, event sampling, and indexing best practices.

17. Q: Which Splunk log file contains internal events for each processor?

A: splunkd.log located in the _internal index.

18. Q: What command shows the input status of monitored files?

A: `splunk list inputstatus` or the REST endpoint `/services/admin/inputstatus/TailingProcessor:FileStatus`.

19. Q: Which log file contains the search execution details?

A: search.log, stored in SPLUNK_HOME/var/run/splunk/dispatch/<sid>/

20. Q: Which component determines the event boundary and performs timestamp extraction?

A: The aggregator processor in the merging pipeline.

21. Q: How can you improve search performance for users?

A: By using base searches, search macros, event sampling, and indexing best practices.

22. Q: Where can the status of queues and pipelines be found?

A: In metrics.log under group=queue or group=pipeline.

23. Q: What is the function of metrics.log in identifying indexing problems?

A: It shows queue sizes, CPU usage, throughput, and blocked queues which can help pinpoint bottlenecks.

Troubleshooting Splunk Q&A (Modules 1-7)

24. Q: How can you detect skipped or delayed searches?

A: By checking scheduler.log and looking for 'skipped' entries.

25. Q: How can you improve search performance for users?

A: By using base searches, search macros, event sampling, and indexing best practices.

26. Q: What component tracks indexing volume against license usage?

A: The License Manager and its associated logs.

27. Q: What file is edited for advanced deployment configurations?

A: serverclass.conf on the deployment server.

28. Q: What file is edited for advanced deployment configurations?

A: serverclass.conf on the deployment server.

29. Q: How can you detect skipped or delayed searches?

A: By checking scheduler.log and looking for 'skipped' entries.

30. Q: What does a 'blocked=true' status in a queue indicate?

A: That the queue is full and processing is delayed or halted.

31. Q: What are symptoms of poor search performance?

A: Long dispatch times, low completion percentages, or skipped searches.

32. Q: Where can the status of queues and pipelines be found?

A: In metrics.log under group=queue or group=pipeline.

33. Q: What does a 'blocked=true' status in a queue indicate?

A: That the queue is full and processing is delayed or halted.

34. Q: What does a 'blocked=true' status in a queue indicate?

A: That the queue is full and processing is delayed or halted.

35. Q: Where can the status of queues and pipelines be found?

A: In metrics.log under group=queue or group=pipeline.

36. Q: Which component determines the event boundary and performs timestamp extraction?

A: The aggregator processor in the merging pipeline.

37. Q: How can you detect skipped or delayed searches?

A: By checking scheduler.log and looking for 'skipped' entries.

38. Q: Which Splunk log file contains internal events for each processor?

A: splunkd.log located in the _internal index.

39. Q: Which Splunk log file contains internal events for each processor?

A: splunkd.log located in the _internal index.

40. Q: How can you improve search performance for users?

A: By using base searches, search macros, event sampling, and indexing best practices.

41. Q: What is the function of metrics.log in identifying indexing problems?

A: It shows queue sizes, CPU usage, throughput, and blocked queues which can help pinpoint bottlenecks.

42. Q: What logs provide insight into deployment server activity?

A: Logs from the DS component in _internal index.

43. Q: Which log file contains the search execution details?

A: search.log, stored in SPLUNK_HOME/var/run/splunk/dispatch/<sid>/

44. Q: Which log file contains the search execution details?

A: search.log, stored in SPLUNK_HOME/var/run/splunk/dispatch/<sid>/

45. Q: Where can the status of queues and pipelines be found?

A: In metrics.log under group=queue or group=pipeline.

46. Q: Where do you find errors related to search artifacts or permissions?

A: In the splunkd.log or audit.log.

Troubleshooting Splunk Q&A (Modules 1-7)

47. Q: What is the fishbucket and its role?

A: It stores CRC and seek pointers to prevent re-indexing files.

48. Q: Which component determines the event boundary and performs timestamp extraction?

A: The aggregator processor in the merging pipeline.

49. Q: How can duplicate indexing be detected?

A: By checking splunkd logs for WatchedFile component and comparing _indextime values.

50. Q: How does license overuse manifest in Splunk?

A: You'll see warnings in license.log, and Splunk will enter a restricted search mode.

51. Q: How can you detect skipped or delayed searches?

A: By checking scheduler.log and looking for 'skipped' entries.

52. Q: Which log file contains the search execution details?

A: search.log, stored in SPLUNK_HOME/var/run/splunk/dispatch/<sid>/

53. Q: What component tracks indexing volume against license usage?

A: The License Manager and its associated logs.

54. Q: What is the function of metrics.log in identifying indexing problems?

A: It shows queue sizes, CPU usage, throughput, and blocked queues which can help pinpoint bottlenecks.

55. Q: Which component determines the event boundary and performs timestamp extraction?

A: The aggregator processor in the merging pipeline.

56. Q: Where can you verify user roles and capabilities?

A: In authorize.conf and via the Splunk Web UI under Settings > Access Controls.

57. Q: Where can you verify user roles and capabilities?

A: In authorize.conf and via the Splunk Web UI under Settings > Access Controls.

58. Q: Which component determines the event boundary and performs timestamp extraction?

A: The aggregator processor in the merging pipeline.

59. Q: What file is edited for advanced deployment configurations?

A: serverclass.conf on the deployment server.

60. Q: Where can you verify user roles and capabilities?

A: In authorize.conf and via the Splunk Web UI under Settings > Access Controls.

61. Q: What are symptoms of poor search performance?

A: Long dispatch times, low completion percentages, or skipped searches.

62. Q: How does license overuse manifest in Splunk?

A: You'll see warnings in license.log, and Splunk will enter a restricted search mode.

63. Q: What is the purpose of Splunk's diag tool?

A: It gathers logs, configurations, and system information to help diagnose issues and is anonymized before sharing with Splunk.

64. Q: What is the purpose of Splunk's diag tool?

A: It gathers logs, configurations, and system information to help diagnose issues and is anonymized before sharing with Splunk.

65. Q: What does a 'blocked=true' status in a queue indicate?

A: That the queue is full and processing is delayed or halted.

66. Q: Which log file contains the search execution details?

A: search.log, stored in SPLUNK_HOME/var/run/splunk/dispatch/<sid>/

67. Q: What is the function of metrics.log in identifying indexing problems?

A: It shows queue sizes, CPU usage, throughput, and blocked queues which can help pinpoint bottlenecks.

68. Q: What component helps distribute search loads across peers?

A: The Search Head and Search Peer topology.

Troubleshooting Splunk Q&A (Modules 1-7)

69. Q: Which component determines the event boundary and performs timestamp extraction?

A: The aggregator processor in the merging pipeline.

70. Q: Which Splunk log file contains internal events for each processor?

A: splunkd.log located in the _internal index.

71. Q: What component helps distribute search loads across peers?

A: The Search Head and Search Peer topology.

72. Q: Which component determines the event boundary and performs timestamp extraction?

A: The aggregator processor in the merging pipeline.

73. Q: What is the purpose of Splunk's diag tool?

A: It gathers logs, configurations, and system information to help diagnose issues and is anonymized before sharing with Splunk.

74. Q: Where can the status of queues and pipelines be found?

A: In metrics.log under group=queue or group=pipeline.

75. Q: What is the function of metrics.log in identifying indexing problems?

A: It shows queue sizes, CPU usage, throughput, and blocked queues which can help pinpoint bottlenecks.

76. Q: Which Splunk log file contains internal events for each processor?

A: splunkd.log located in the _internal index.

77. Q: Which log file contains the search execution details?

A: search.log, stored in SPLUNK_HOME/var/run/splunk/dispatch/<sid>/

78. Q: Which log file contains the search execution details?

A: search.log, stored in SPLUNK_HOME/var/run/splunk/dispatch/<sid>/

79. Q: Which log file contains the search execution details?

A: search.log, stored in SPLUNK_HOME/var/run/splunk/dispatch/<sid>/

Troubleshooting Splunk Q&A (Modules 1-7)

80. Q: Where can you verify user roles and capabilities?

A: In authorize.conf and via the Splunk Web UI under Settings > Access Controls.

81. Q: Where can the status of queues and pipelines be found?

A: In metrics.log under group=queue or group=pipeline.

82. Q: Where can you verify user roles and capabilities?

A: In authorize.conf and via the Splunk Web UI under Settings > Access Controls.

83. Q: What logs provide insight into deployment server activity?

A: Logs from the DS component in _internal index.

84. Q: What does a 'blocked=true' status in a queue indicate?

A: That the queue is full and processing is delayed or halted.

85. Q: What is the fishbucket and its role?

A: It stores CRC and seek pointers to prevent re-indexing files.

86. Q: What are symptoms of poor search performance?

A: Long dispatch times, low completion percentages, or skipped searches.

87. Q: What logs provide insight into deployment server activity?

A: Logs from the DS component in _internal index.

88. Q: Where can you verify user roles and capabilities?

A: In authorize.conf and via the Splunk Web UI under Settings > Access Controls.

89. Q: What does a 'blocked=true' status in a queue indicate?

A: That the queue is full and processing is delayed or halted.

90. Q: What logs provide insight into deployment server activity?

A: Logs from the DS component in _internal index.

91. Q: What are symptoms of poor search performance?

A: Long dispatch times, low completion percentages, or skipped searches.

92. Q: Where can you verify user roles and capabilities?

A: In authorize.conf and via the Splunk Web UI under Settings > Access Controls.

93. Q: How can duplicate indexing be detected?

A: By checking splunkd logs for WatchedFile component and comparing _indextime values.

94. Q: What is the purpose of Splunk's diag tool?

A: It gathers logs, configurations, and system information to help diagnose issues and is anonymized before sharing with Splunk.

95. Q: How can you detect skipped or delayed searches?

A: By checking scheduler.log and looking for 'skipped' entries.

96. Q: What component tracks indexing volume against license usage?

A: The License Manager and its associated logs.

97. Q: Where do you find errors related to search artifacts or permissions?

A: In the splunkd.log or audit.log.

98. Q: What are signs that apps are not deploying properly to clients?

A: Clients may not contact the correct DS, or whitelist/blacklist settings might be incorrect.

99. Q: Which log file contains the search execution details?

A: search.log, stored in SPLUNK_HOME/var/run/splunk/dispatch/<sid>/

100. Q: What are symptoms of poor search performance?

A: Long dispatch times, low completion percentages, or skipped searches.