Splunk Data Admin Q&A (Modules 5, 6, 7, 8, 10)

1. Q: How do deployment clients connect to a deployment server?

A: Using the splunk set deploy-poll <deploymentServer:port> command.

2. Q: What are the four phases of the Splunk distributed model?

A: Input, Parsing, Indexing, and Search.

3. Q: Where are Splunk configuration files stored?

A: Under SPLUNK_HOME/etc directory.

4. Q: What does a deployment server do in Splunk?

A: Centrally manages configuration apps and distributes them to deployment clients.

5. Q: What command is used to validate configuration files in Splunk?

A: splunk btool <conf_file> list

6. Q: What port does Splunk use for receiving forwarded data by default?

A: Port 9997.

7. Q: What are the four phases of the Splunk distributed model?

A: Input, Parsing, Indexing, and Search.

8. Q: What port does Splunk use for receiving forwarded data by default?

A: Port 9997.

9. Q: What metadata is set during the input phase?

A: source, sourcetype, host, and index.

10. Q: What metadata is set during the input phase?

A: source, sourcetype, host, and index.

11. Q: What are the four phases of the Splunk distributed model?

A: Input, Parsing, Indexing, and Search.

12. Q: Where are Splunk configuration files stored?

A: Under SPLUNK_HOME/etc directory.

13. Q: What is a Heavy Forwarder (HF)?

A: A full Splunk Enterprise instance that can parse and route data before forwarding.

14. Q: What is the default index if none is specified during data input?

A: The 'main' index.

15. Q: What are the four phases of the Splunk distributed model?

A: Input, Parsing, Indexing, and Search.

16. Q: What port does Splunk use for receiving forwarded data by default?

A: Port 9997.

17. Q: What file is used to define field extractions and transformations?

A: transforms.conf.

18. Q: What is a Heavy Forwarder (HF)?

A: A full Splunk Enterprise instance that can parse and route data before forwarding.

19. Q: Where is the best place to test data configuration before sending to production?

A: In a test or deployment server using sample logs.

20. Q: What port does Splunk use for receiving forwarded data by default?

A: Port 9997.

21. Q: What is a Heavy Forwarder (HF)?

A: A full Splunk Enterprise instance that can parse and route data before forwarding.

22. Q: Where is the best place to test data configuration before sending to production?

A: In a test or deployment server using sample logs.

23. Q: What port does Splunk use for receiving forwarded data by default?

A: Port 9997.

Splunk Data Admin Q&A (Modules 5, 6, 7, 8, 10)

24. Q: What file is used to define field extractions and transformations?

A: transforms.conf.

25. Q: What configuration file defines where data should be forwarded?

A: outputs.conf

26. Q: What does a deployment server do in Splunk?

A: Centrally manages configuration apps and distributes them to deployment clients.

27. Q: How is a heavy forwarder different from a universal forwarder?

A: HF can parse data, support complex routing, and has a GUI; UF is lightweight with no parsing.

28. Q: What is a Heavy Forwarder (HF)?

A: A full Splunk Enterprise instance that can parse and route data before forwarding.

29. Q: Where are Splunk configuration files stored?

A: Under SPLUNK_HOME/etc directory.

30. Q: Where is the best place to test data configuration before sending to production?

A: In a test or deployment server using sample logs.

31. Q: What command is used to configure a forwarder to send data?

A: splunk add forward-server <indexer:port>

32. Q: Where are deployment apps stored on the deployment server?

A: SPLUNK_HOME/etc/deployment-apps/

33. Q: How do deployment clients connect to a deployment server?

A: Using the splunk set deploy-poll <deploymentServer:port> command.

34. Q: What command is used to validate configuration files in Splunk?

A: splunk btool <conf_file> list

35. Q: How is a heavy forwarder different from a universal forwarder?

A: HF can parse data, support complex routing, and has a GUI; UF is lightweight with no parsing.

36. Q: What are the four phases of the Splunk distributed model?

A: Input, Parsing, Indexing, and Search.

37. Q: Where are Splunk configuration files stored?

A: Under SPLUNK_HOME/etc directory.

38. Q: What tool is used to manage forwarders centrally?

A: Splunk Deployment Server.

39. Q: What is the purpose of the serverclass.conf file?

A: Defines which deployment clients receive which apps.

40. Q: Where is the best place to test data configuration before sending to production?

A: In a test or deployment server using sample logs.

41. Q: How is a heavy forwarder different from a universal forwarder?

A: HF can parse data, support complex routing, and has a GUI; UF is lightweight with no parsing.

42. Q: What file is used to define field extractions and transformations?

A: transforms.conf.

43. Q: What type of data manipulation can be done at index-time?

A: Masking sensitive data, adjusting timestamps, or altering field names.

44. Q: Where are Splunk configuration files stored?

A: Under SPLUNK_HOME/etc directory.

45. Q: Where are deployment apps stored on the deployment server?

A: SPLUNK_HOME/etc/deployment-apps/

46. Q: Where are Splunk configuration files stored?

A: Under SPLUNK_HOME/etc directory.

Splunk Data Admin Q&A (Modules 5, 6, 7, 8, 10)

47. Q: What are the default queue sizes when useACK=true in outputs.conf?

A: Output queue: 7 MB, Wait queue: 21 MB.

48. Q: What tool is used to manage forwarders centrally?

A: Splunk Deployment Server.

49. Q: What is the purpose of the serverclass.conf file?

A: Defines which deployment clients receive which apps.

50. Q: What does a deployment server do in Splunk?

A: Centrally manages configuration apps and distributes them to deployment clients.

51. Q: What type of data manipulation can be done at index-time?

A: Masking sensitive data, adjusting timestamps, or altering field names.

52. Q: What configuration file defines where data should be forwarded?

A: outputs.conf

53. Q: What does a deployment server do in Splunk?

A: Centrally manages configuration apps and distributes them to deployment clients.

54. Q: What command is used to validate configuration files in Splunk?

A: splunk btool <conf_file> list

55. Q: What type of data manipulation can be done at index-time?

A: Masking sensitive data, adjusting timestamps, or altering field names.

56. Q: What type of data manipulation can be done at index-time?

A: Masking sensitive data, adjusting timestamps, or altering field names.

57. Q: What is the purpose of the serverclass.conf file?

A: Defines which deployment clients receive which apps.

58. Q: What tool is used to manage forwarders centrally?

A: Splunk Deployment Server.

59. Q: What is a Heavy Forwarder (HF)?

A: A full Splunk Enterprise instance that can parse and route data before forwarding.

60. Q: What type of data manipulation can be done at index-time?

A: Masking sensitive data, adjusting timestamps, or altering field names.

61. Q: Where are Splunk configuration files stored?

A: Under SPLUNK_HOME/etc directory.

62. Q: What tool is used to manage forwarders centrally?

A: Splunk Deployment Server.

63. Q: What tool is used to manage forwarders centrally?

A: Splunk Deployment Server.

64. Q: What is a Universal Forwarder (UF)?

A: A lightweight Splunk agent that collects and forwards data to indexers.

65. Q: What is the default index if none is specified during data input?

A: The 'main' index.

66. Q: What does a deployment server do in Splunk?

A: Centrally manages configuration apps and distributes them to deployment clients.

67. Q: What are the default queue sizes when useACK=true in outputs.conf?

A: Output queue: 7 MB, Wait queue: 21 MB.

68. Q: How is a heavy forwarder different from a universal forwarder?

A: HF can parse data, support complex routing, and has a GUI; UF is lightweight with no parsing.

69. Q: What types of data inputs does Splunk support?

A: Files/directories, network data, script output, Windows logs, and HTTP Event Collector.

Splunk Data Admin Q&A (Modules 5, 6, 7, 8, 10)

70. Q: What file is used to define field extractions and transformations?

A: transforms.conf.

71. Q: What is a Universal Forwarder (UF)?

A: A lightweight Splunk agent that collects and forwards data to indexers.

72. Q: What is a good reason to modify props.conf?

A: To control line breaking, timestamp extraction, or character encoding.

73. Q: What are the four phases of the Splunk distributed model?

A: Input, Parsing, Indexing, and Search.

74. Q: What file is used to define field extractions and transformations?

A: transforms.conf.

75. Q: What configuration file defines where data should be forwarded?

A: outputs.conf

76. Q: What is a Heavy Forwarder (HF)?

A: A full Splunk Enterprise instance that can parse and route data before forwarding.

77. Q: How do deployment clients connect to a deployment server?

A: Using the splunk set deploy-poll <deploymentServer:port> command.

78. Q: What file is used to define field extractions and transformations?

A: transforms.conf.

79. Q: What type of data manipulation can be done at index-time?

A: Masking sensitive data, adjusting timestamps, or altering field names.

80. Q: Where is the best place to test data configuration before sending to production?

A: In a test or deployment server using sample logs.

81. Q: Where are deployment apps stored on the deployment server?

A: SPLUNK_HOME/etc/deployment-apps/

82. Q: What tool is used to manage forwarders centrally?

A: Splunk Deployment Server.

83. Q: What type of data manipulation can be done at index-time?

A: Masking sensitive data, adjusting timestamps, or altering field names.

84. Q: How do deployment clients connect to a deployment server?

A: Using the splunk set deploy-poll <deploymentServer:port> command.

85. Q: What is a good reason to modify props.conf?

A: To control line breaking, timestamp extraction, or character encoding.

86. Q: What type of data manipulation can be done at index-time?

A: Masking sensitive data, adjusting timestamps, or altering field names.

87. Q: What is a good reason to modify props.conf?

A: To control line breaking, timestamp extraction, or character encoding.

88. Q: What is the purpose of the serverclass.conf file?

A: Defines which deployment clients receive which apps.

89. Q: What configuration file defines where data should be forwarded?

A: outputs.conf

90. Q: How do deployment clients connect to a deployment server?

A: Using the splunk set deploy-poll <deploymentServer:port> command.

91. Q: What is a Universal Forwarder (UF)?

A: A lightweight Splunk agent that collects and forwards data to indexers.

92. Q: What command is used to configure a forwarder to send data?

A: splunk add forward-server <indexer:port>

Splunk Data Admin Q&A (Modules 5, 6, 7, 8, 10)

93. Q: What command is used to configure a forwarder to send data?

A: splunk add forward-server <indexer:port>

94. Q: What is a Heavy Forwarder (HF)?

A: A full Splunk Enterprise instance that can parse and route data before forwarding.

95. Q: What is a Universal Forwarder (UF)?

A: A lightweight Splunk agent that collects and forwards data to indexers.

96. Q: What metadata is set during the input phase?

A: source, sourcetype, host, and index.

97. Q: What port does Splunk use for receiving forwarded data by default?

A: Port 9997.

98. Q: What configuration file defines where data should be forwarded?

A: outputs.conf

99. Q: What is the default index if none is specified during data input?

A: The 'main' index.

100. Q: What is a Heavy Forwarder (HF)?

A: A full Splunk Enterprise instance that can parse and route data before forwarding.