Splunk Q&A (Modules 1, 3, 4, 6, 7)

Q: What percentage of raw data size does the indexed data typically consume?

A: Approximately 50% (15% for rawdata and 35% for index files).

Q: What are the two main types of indexes in Splunk?

A: Event indexes and metric indexes.

Q: What is the reference specification for an indexer in Splunk?

A: 12 CPU cores, 12 GB RAM, 800+ IOPS, and RAID 1+0 disk configuration.

Q: Why is identifying use cases important in Splunk deployment planning?

A: Use cases help define what users need from Splunk, which influences architecture, data ingestion, and app selection.

Q: What are the two main types of indexes in Splunk?

A: Event indexes and metric indexes.

Q: What access control best practice is recommended for integrating with LDAP?

A: Mapping LDAP groups to Splunk roles with defined capabilities and filters.

Q: What percentage of raw data size does the indexed data typically consume?

A: Approximately 50% (15% for rawdata and 35% for index files).

Q: What are the main responsibilities of a Splunk Architect?

A: Capacity planning, deployment strategy creation, backup and DR strategy implementation, and documentation of architecture.

Splunk Q&A (Modules 1, 3, 4, 6, 7)

Q: Why is identifying use cases important in Splunk deployment planning?

A: Use cases help define what users need from Splunk, which influences architecture, data ingestion, and app selection.

Q: Which authentication methods can Splunk integrate with?

A: LDAP, SAML, ProxySSO, and scripted authentication (e.g., PAM or RADIUS).

Q: Why is identifying use cases important in Splunk deployment planning?

A: Use cases help define what users need from Splunk, which influences architecture, data ingestion, and app selection.

Q: What is the reference specification for an indexer in Splunk?

A: 12 CPU cores, 12 GB RAM, 800+ IOPS, and RAID 1+0 disk configuration.

Q: Why is identifying use cases important in Splunk deployment planning?

A: Use cases help define what users need from Splunk, which influences architecture, data ingestion, and app selection.

Q: Why is identifying use cases important in Splunk deployment planning?

A: Use cases help define what users need from Splunk, which influences architecture, data ingestion, and app selection.

Q: What percentage of raw data size does the indexed data typically consume?

A: Approximately 50% (15% for rawdata and 35% for index files).

Q: How does a deployment server operate?

A: It manages configurations for deployment clients using a pull model.

Q: What percentage of raw data size does the indexed data typically consume?

A: Approximately 50% (15% for rawdata and 35% for index files).

Q: Why is identifying use cases important in Splunk deployment planning?

A: Use cases help define what users need from Splunk, which influences architecture, data ingestion, and app selection.

Q: What are the main responsibilities of a Splunk Architect?

A: Capacity planning, deployment strategy creation, backup and DR strategy implementation, and documentation of architecture.

Q: What are the two main types of indexes in Splunk?

A: Event indexes and metric indexes.

Q: What percentage of raw data size does the indexed data typically consume?

A: Approximately 50% (15% for rawdata and 35% for index files).

Q: What access control best practice is recommended for integrating with LDAP?

A: Mapping LDAP groups to Splunk roles with defined capabilities and filters.

Q: What access control best practice is recommended for integrating with LDAP?

A: Mapping LDAP groups to Splunk roles with defined capabilities and filters.

Q: What tool is used to understand Buttercup Games' network topology?

A: A network topology diagram provided in the deployment documentation.

Q: How does a deployment server operate?

A: It manages configurations for deployment clients using a pull model.

Q: What is the reference specification for an indexer in Splunk?

A: 12 CPU cores, 12 GB RAM, 800+ IOPS, and RAID 1+0 disk configuration.

Q: What percentage of raw data size does the indexed data typically consume?

A: Approximately 50% (15% for rawdata and 35% for index files).

Q: What tool is used to understand Buttercup Games' network topology?

A: A network topology diagram provided in the deployment documentation.

Q: What is the reference specification for an indexer in Splunk?

A: 12 CPU cores, 12 GB RAM, 800+ IOPS, and RAID 1+0 disk configuration.

Q: What are the two main types of indexes in Splunk?

A: Event indexes and metric indexes.

Q: What are the two main types of indexes in Splunk?

A: Event indexes and metric indexes.

Q: What are the two main types of indexes in Splunk?

A: Event indexes and metric indexes.

Splunk Q&A (Modules 1, 3, 4, 6, 7)

Q: Which authentication methods can Splunk integrate with?

A: LDAP, SAML, ProxySSO, and scripted authentication (e.g., PAM or RADIUS).

Q: What are the two main types of indexes in Splunk?

A: Event indexes and metric indexes.

Q: What tool is used to understand Buttercup Games' network topology?

A: A network topology diagram provided in the deployment documentation.

Q: What is the reference specification for an indexer in Splunk?

A: 12 CPU cores, 12 GB RAM, 800+ IOPS, and RAID 1+0 disk configuration.

Q: What is the reference specification for an indexer in Splunk?

A: 12 CPU cores, 12 GB RAM, 800+ IOPS, and RAID 1+0 disk configuration.

Q: What tool is used to understand Buttercup Games' network topology?

A: A network topology diagram provided in the deployment documentation.

Q: Why is identifying use cases important in Splunk deployment planning?

A: Use cases help define what users need from Splunk, which influences architecture, data ingestion, and app selection.

Q: What is the reference specification for an indexer in Splunk?

A: 12 CPU cores, 12 GB RAM, 800+ IOPS, and RAID 1+0 disk configuration.

Q: What percentage of raw data size does the indexed data typically consume?

A: Approximately 50% (15% for rawdata and 35% for index files).

Q: How does a deployment server operate?

A: It manages configurations for deployment clients using a pull model.

Q: What is the reference specification for an indexer in Splunk?

A: 12 CPU cores, 12 GB RAM, 800+ IOPS, and RAID 1+0 disk configuration.

Q: How does a deployment server operate?

A: It manages configurations for deployment clients using a pull model.

Q: What are the two main types of indexes in Splunk?

A: Event indexes and metric indexes.

Q: What is the reference specification for an indexer in Splunk?

A: 12 CPU cores, 12 GB RAM, 800+ IOPS, and RAID 1+0 disk configuration.

Q: What is the difference between a universal forwarder and a heavy forwarder?

A: A universal forwarder is lightweight and only forwards data, while a heavy forwarder can parse and index data.

Q: What access control best practice is recommended for integrating with LDAP?

A: Mapping LDAP groups to Splunk roles with defined capabilities and filters.

Q: What are the main responsibilities of a Splunk Architect?

A: Capacity planning, deployment strategy creation, backup and DR strategy implementation, and documentation of architecture.

Q: What percentage of raw data size does the indexed data typically consume?

A: Approximately 50% (15% for rawdata and 35% for index files).

Q: What are the two main types of indexes in Splunk?

A: Event indexes and metric indexes.

Q: What access control best practice is recommended for integrating with LDAP?

A: Mapping LDAP groups to Splunk roles with defined capabilities and filters.

Q: What percentage of raw data size does the indexed data typically consume?

A: Approximately 50% (15% for rawdata and 35% for index files).

Q: What is the difference between a universal forwarder and a heavy forwarder?

A: A universal forwarder is lightweight and only forwards data, while a heavy forwarder can parse and index data.

Q: What is the difference between a universal forwarder and a heavy forwarder?

A: A universal forwarder is lightweight and only forwards data, while a heavy forwarder can parse and index data.

Q: Why is identifying use cases important in Splunk deployment planning?

A: Use cases help define what users need from Splunk, which influences architecture, data ingestion, and app selection.

Splunk Q&A (Modules 1, 3, 4, 6, 7)

Q: What percentage of raw data size does the indexed data typically consume?

A: Approximately 50% (15% for rawdata and 35% for index files).

Q: What is the reference specification for an indexer in Splunk?

A: 12 CPU cores, 12 GB RAM, 800+ IOPS, and RAID 1+0 disk configuration.

Q: Why is identifying use cases important in Splunk deployment planning?

A: Use cases help define what users need from Splunk, which influences architecture, data ingestion, and app selection.

Q: What are the main responsibilities of a Splunk Architect?

A: Capacity planning, deployment strategy creation, backup and DR strategy implementation, and documentation of architecture.

Q: What are the two main types of indexes in Splunk?

A: Event indexes and metric indexes.

Q: What is the difference between a universal forwarder and a heavy forwarder?

A: A universal forwarder is lightweight and only forwards data, while a heavy forwarder can parse and index data.

Q: What is the reference specification for an indexer in Splunk?

A: 12 CPU cores, 12 GB RAM, 800+ IOPS, and RAID 1+0 disk configuration.

Q: What is the difference between a universal forwarder and a heavy forwarder?

A: A universal forwarder is lightweight and only forwards data, while a heavy forwarder can parse and index

data.

Q: How does a deployment server operate?

A: It manages configurations for deployment clients using a pull model.

Q: What are the two main types of indexes in Splunk?

A: Event indexes and metric indexes.

Q: What is the reference specification for an indexer in Splunk?

A: 12 CPU cores, 12 GB RAM, 800+ IOPS, and RAID 1+0 disk configuration.

Q: What are the main responsibilities of a Splunk Architect?

A: Capacity planning, deployment strategy creation, backup and DR strategy implementation, and documentation of architecture.

Q: Why is identifying use cases important in Splunk deployment planning?

A: Use cases help define what users need from Splunk, which influences architecture, data ingestion, and app selection.

Q: What are the two main types of indexes in Splunk?

A: Event indexes and metric indexes.

Q: What is the difference between a universal forwarder and a heavy forwarder?

A: A universal forwarder is lightweight and only forwards data, while a heavy forwarder can parse and index data.

Splunk Q&A (Modules 1, 3, 4, 6, 7)

Q: What is the difference between a universal forwarder and a heavy forwarder?

A: A universal forwarder is lightweight and only forwards data, while a heavy forwarder can parse and index data.

Q: How does a deployment server operate?

A: It manages configurations for deployment clients using a pull model.

Q: What are the two main types of indexes in Splunk?

A: Event indexes and metric indexes.

Q: What percentage of raw data size does the indexed data typically consume?

A: Approximately 50% (15% for rawdata and 35% for index files).

Q: What percentage of raw data size does the indexed data typically consume?

A: Approximately 50% (15% for rawdata and 35% for index files).

Q: What access control best practice is recommended for integrating with LDAP?

A: Mapping LDAP groups to Splunk roles with defined capabilities and filters.

Q: What tool is used to understand Buttercup Games' network topology?

A: A network topology diagram provided in the deployment documentation.

Q: How does a deployment server operate?

A: It manages configurations for deployment clients using a pull model.

Q: What is the difference between a universal forwarder and a heavy forwarder?

A: A universal forwarder is lightweight and only forwards data, while a heavy forwarder can parse and index data.

Q: How does a deployment server operate?

A: It manages configurations for deployment clients using a pull model.

Q: What is the difference between a universal forwarder and a heavy forwarder?

A: A universal forwarder is lightweight and only forwards data, while a heavy forwarder can parse and index data.

Q: Why is identifying use cases important in Splunk deployment planning?

A: Use cases help define what users need from Splunk, which influences architecture, data ingestion, and app selection.

Q: Why is identifying use cases important in Splunk deployment planning?

A: Use cases help define what users need from Splunk, which influences architecture, data ingestion, and app selection.

Q: What is the difference between a universal forwarder and a heavy forwarder?

A: A universal forwarder is lightweight and only forwards data, while a heavy forwarder can parse and index data.