



Free Questions for [SPLK-3003](#) by [certscare](#)

Shared by [Stevenson](#) on [09-08-2024](#)

For More Free Questions and Preparation Resources

[Check the Links on Last Page](#)

Question 1

Question Type: MultipleChoice

A customer wants to understand how Splunk bucket types (hot, warm, cold) impact search performance within their environment. Their indexers have a single storage device for all data

a. What is the proper message to communicate to the customer?

Options:

- A-** The bucket types (hot, warm, or cold) have the same search performance characteristics within the customer's environment.
- B-** While hot, warm, and cold buckets have the same search performance characteristics within the customer's environment, due to their optimized structure, the thawed buckets are the most performant.
- C-** Searching hot and warm buckets result in best performance because by default the cold buckets are miniaturized by removing TSIDX files to save on storage cost.
- D-** Because the cold buckets are written to a cheaper/slower storage volume, they will be slower to search compared to hot and warm buckets which are written to Solid State Disk (SSD).

Answer:

D

Question 2

Question Type: MultipleChoice

A [script://] input sends data to a Splunk forwarder using which method?

Options:

- A- UDP stream
- B- TCP stream
- C- Temporary file
- D- STDOUT/STDERR

Answer:

C

Question 3

Question Type: MultipleChoice

A customer has a search cluster (SHC) of six members split evenly between two data centers (DC). The customer is concerned with network connectivity between the two DCs due to frequent outages. Which of the following is true as it relates to SHC resiliency when a network outage occurs between the two DCs?

Options:

- A-** The SHC will function as expected as the SHC deployer will become the new captain until the network communication is restored.
- B-** The SHC will stop all scheduled search activity within the SHC.
- C-** The SHC will function as expected as the minimum required number of nodes for a SHC is 3.
- D-** The SHC will function as expected as the SHC captain will fall back to previous active captain in the remaining site.

Answer:

D

Question 4

Question Type: MultipleChoice

A customer wants to implement LDAP because managing local Splunk users is becoming too much of an overhead. What configuration details are needed from the customer to implement LDAP authentication?

Options:

A- API: Python script with PAM/RADIUS details.

B- LDAP server: port, bind user credentials, path/to/groups, path/to/user.

C- LDAP server: port, bind user credentials, base DN for groups, base DN for users.

D- LDAP REST details, base DN for groups, base DN for users.

Answer:

C

Question 5

Question Type: MultipleChoice

A site from a multi-site indexer cluster needs to be decommissioned. Which of the following actions must be taken?

Options:

- A- Nothing. Decommissioning a site is not possible.
- B- Create an alias for where the new data should be sent.
- C- Remove the site from the list of available sites.
- D- Remove the site from the list of available sites and create an alias for where the new data should be sent.

Answer:

D

Question 6

Question Type: MultipleChoice

When a bucket rolls from cold to frozen on a clustered indexer, which of the following scenarios occurs?

Options:

- A- All replicated copies will be rolled to frozen; original copies will remain.
- B- Replicated copies of the bucket will remain on all other indexers and the Cluster Master (CM) assigns a new primary bucket.
- C- The bucket rolls to frozen on all clustered indexers simultaneously.

D- Nothing. Replicated copies of the bucket will remain on all other indexers until a local retention rule causes it to roll.

Answer:

B

Question 7

Question Type: MultipleChoice

A customer has a new set of hardware to replace their aging indexers. What method would reduce the amount of bucket replication operations during the migration process?

Options:

- A-** Disable the indexing ports on the old indexers.
- B-** Disable replication ports on the old indexers.
- C-** Put the old indexers into manual detention.
- D-** Put the old indexers into automatic detention.

Answer:

D

Question 8

Question Type: MultipleChoice

Which configuration item should be set to false to significantly improve data ingestion performance?

Options:

A- AUTO_KV_JSON

B- BREAK_ONLY_BEFORE_DATE

C- SHOULD_LINEMERGE

D- ANNOTATE_PUNCT

Answer:

C

Question 9

Question Type: MultipleChoice

Which of the following processor occur in the indexing pipeline?

Options:

- A- tcp out, syslog out
- B- Regex replacement, annotator
- C- Aggregator
- D- UTF-8, linebreaker, header

Answer:

A

Question 10

Question Type: MultipleChoice

What is the Splunk PS recommendation when using the deployment server and building deployment apps?

Options:

- A- Carefully design smaller apps with specific configuration that can be reused.
- B- Only deploy Splunk PS base configurations via the deployment server.
- C- Use \$SPLUNK_HOME/etc/system/local configurations on forwarders and only deploy TAs via the deployment server.
- D- Carefully design bigger apps containing multiple configs.

Answer:

B

Question 11

Question Type: MultipleChoice

Which of the following server.conf stanzas indicates the Indexer Discovery feature has not been fully configured (restart pending) on the Master Node?

- A. [indexer_discovery]
pass4SymmKey = \$7\$XcXl1lu3820Jbui14oVe324+mvx6gCKKv6kf2zEaVB6Ie4DcZ647CnLVlFW
- B. [clustering]
mode = master
pass4SymmKey = \$7\$tYTXzke+1r+3DULTHHDUTmYOXdtZJPxm21XwMARrJE20jsmicp9C3ni0
- C. [indexer_discovery]
pass4SymmKey = idxdiscovery
- D. [clustering]
mode = forwarder
pass4SymmKey = \$7\$PU9SBXww63Vz3UJdDYGIN0UrdscRh83ssC2pEpwE6P3gn50iNF094g==

Options:

- A- Option A
- B- Option B
- C- Option C
- D- Option D

Answer:

C

Question 12

Question Type: MultipleChoice

A customer's deployment server is overwhelmed with forwarder connections after adding an additional 1000 clients. The default phone home interval is set to 60 seconds. To reduce the number of connection failures to the DS what is recommended?

Options:

- A- Create a tiered deployment server topology.
- B- Reduce the phone home interval to 6 seconds.
- C- Leave the phone home interval at 60 seconds.
- D- Increase the phone home interval to 600 seconds.

Answer:

A

To Get Premium Files for SPLK-3003 Visit

<https://www.p2pexams.com/products/splk-3003>

For More Free Questions Visit

<https://www.p2pexams.com/splunk/pdf/splk-3003>

