Splunk SPLK-3003 Practice Questions

Shared by Small on 18-08-2026

For More Free Questions and Preparation Resources

Check the Links on Last Page

Question 1

Question Type: MultipleChoice

As a best practice which of the following should be used to ingest data on clustered indexers?

Options:

A- Monitoring (via a process), collecting data (modular inputs) from remote systems/applications
B- Modular inputs, HTTP Event Collector (HEC), inputs.conf monitor stanza
C- Actively listening on ports, monitoring (via a process), collecting data from remote systems/applications
D- splunktcp, splunktcp-ssl, HTTP Event Collector (HEC)

Answer:

B

Question 2

Question Type: MultipleChoice

Which command is most efficient in finding the pass4SymmKey of an index cluster?

Options:

A- find / -name server.conf --print | grep pass4SymKey
B- $SPLUNK_HOME/bin/splunk search | rest splunk_server=local /servicesNS/-/unhash_app/storage/passwords
C- $SPLUNK_HOME/bin/splunk btool server list clustering | grep pass4SymmKey
D- $SPLUNK_HOME/bin/splunk btool clustering list clustering --debug | grep pass4SymmKey

Answer:

D

Question 3

Question Type: MultipleChoice

In which of the following scenarios is a subsearch the most appropriate?

Options:

A- When joining results from multiple indexes.
B- When dynamically filtering hosts.
C- When filtering indexed fields.
D- When joining multiple large datasets.

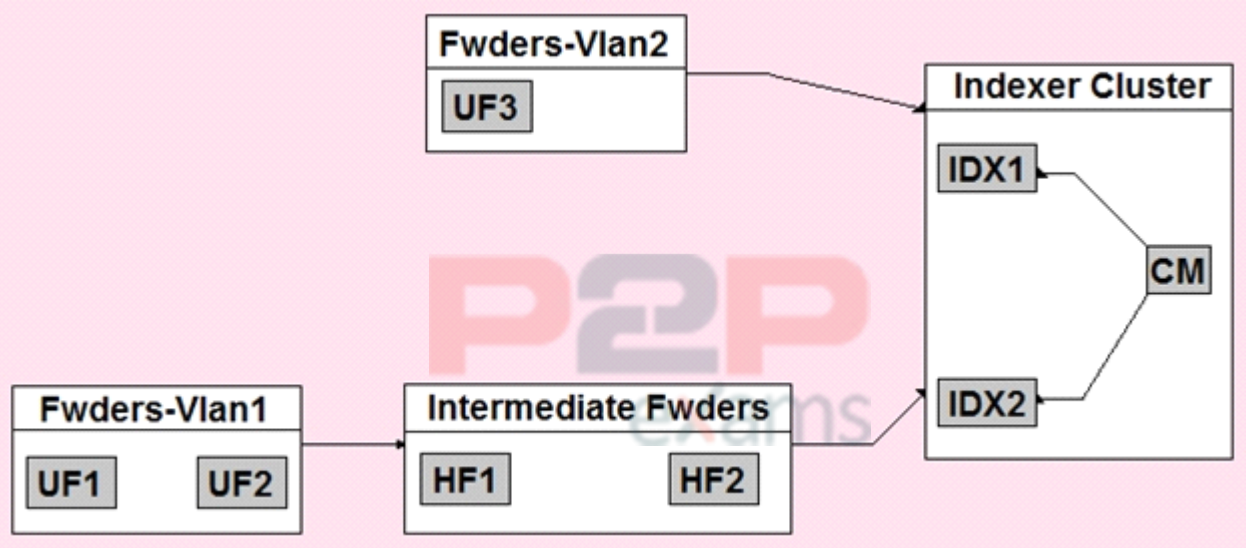
Answer:

A

Question 4

Question Type: MultipleChoice

In the diagrammed environment shown below, the customer would like the data read by the universal forwarders to set an indexed field containing the UF's host name. Where would the parsing configurations need to be installed for this to work?



Options:

A- All universal forwarders.
B- Only the indexers.
C- All heavy forwarders.
D- On all parsing Splunk instances.

Answer:

D

Question 5

Question Type: MultipleChoice

In a single indexer cluster, where should the Monitoring Console (MC) be installed?

Options:

A- Deployer sharing with master cluster.
B- License master that has 50 clients or more.
C- Cluster master node
D- Production Search Head

Answer:

C

Question 6

Question Type: MultipleChoice

The customer has an indexer cluster supporting a wide variety of search needs, including scheduled search, data model acceleration, and summary indexing. Here is an excerpt from the cluster mater's server.conf:

```
[clustering]
replication_factor=2
search_factor=1
summary_replication-false
```

Which strategy represents the minimum and least disruptive change necessary to protect the searchability of the indexer cluster in case of indexer failure?

Options:

A- Enable maintenance mode on the CM to prevent excessive fix-up and bring the failed indexer back online.

B- Leave replication_factor=2, increase search_factor=2 and enable summary_replication.
C- Convert the cluster to multi-site and modify the server.conf to be site_replication_factor=2, site_search_factor=2.
D- Increase replication_factor=3, search_factor=2 to protect the data, and allow there to always be a searchable copy.

Answer:

D

Question 7

Question Type: MultipleChoice

How could a role in which all users must specify an index=clause in all searches be configured?

Options:

A- Set the authorize.conf setting: srchIndexesDefault to no value.
B- Set the authorize.conf setting: srchFilter to no value.
C- Set the authorize.conf setting: srchIndexesAllowed to no value.
D- Set the authorize.conf setting: srchJobsQuota to no value.

Answer:

B

Question 8

Question Type: MultipleChoice

Which option best statements is true, as it pertains to search head clustering (SHC)?

Options:

A- SHC is supported on AIX, Linux, and Windows operating systems.
B- Maximum number of nodes for a SHC is 10.
C- SHC members must run on the same hardware specifications.
D- Minimum number of nodes for a SHC is 5.

Answer:

B

Question 9

Question Type: MultipleChoice

Which of the following is the most efficient search?

Options:

A- index=www status=200 uri=/cart/checkout | append [search index = sales] | stats count, sum(revenue) as total_revenue by session_id | table total_revenue session_id
B- (index=www status=200 uri=/cart/checkout) OR (index=sales) | stats count, sum (revenue) as total_revenue by session_id | table total_revenue session_id
C- index=www | append [search index = sales] | stats count, sum(revenue) as total_revenue by session_id | table total_revenue session_id
D- (index=www) OR (index=sales) | search (index=www status=200 uri=/cart/checkout) OR (index=sales) | stats count, sum(revenue) as total_revenue by session_id | table total_revenue session_id

Answer:

B