Free Questions for SPLK-3003 by vceexamstest

Shared by Stevens on 22-07-2024

For More Free Questions and Preparation Resources

Check the Links on Last Page

Question 1

Question Type: MultipleChoice

In which of the following scenarios should base configurations be used to provide consistent, repeatable, and supportable configurations?

Options:

A- For non-production environments to keep their configurations in sync.

B- To ensure every customer has exactly the same base settings.

C- To provide settings that do not need to be customized to meet customer requirements.

D- To provide settings that can be customized to meet customer requirements.

Answer:

C

Question 2

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.

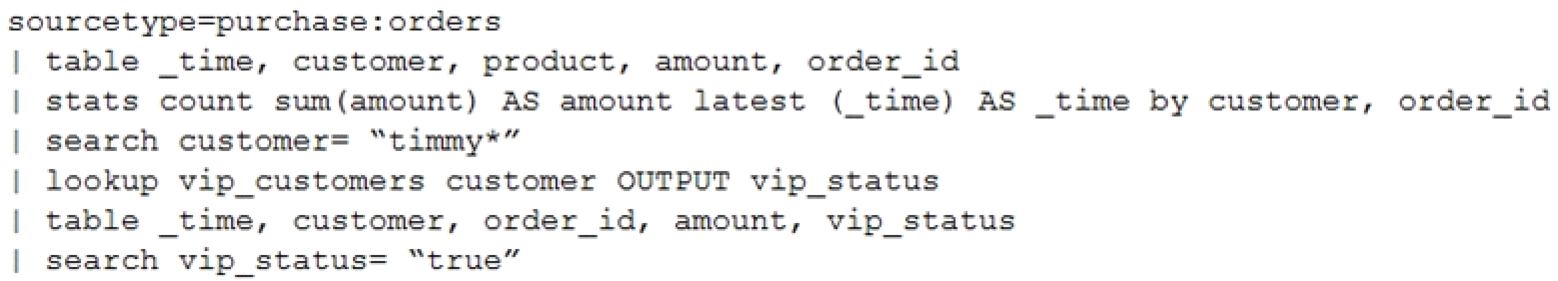
Answer:

B

Question 3

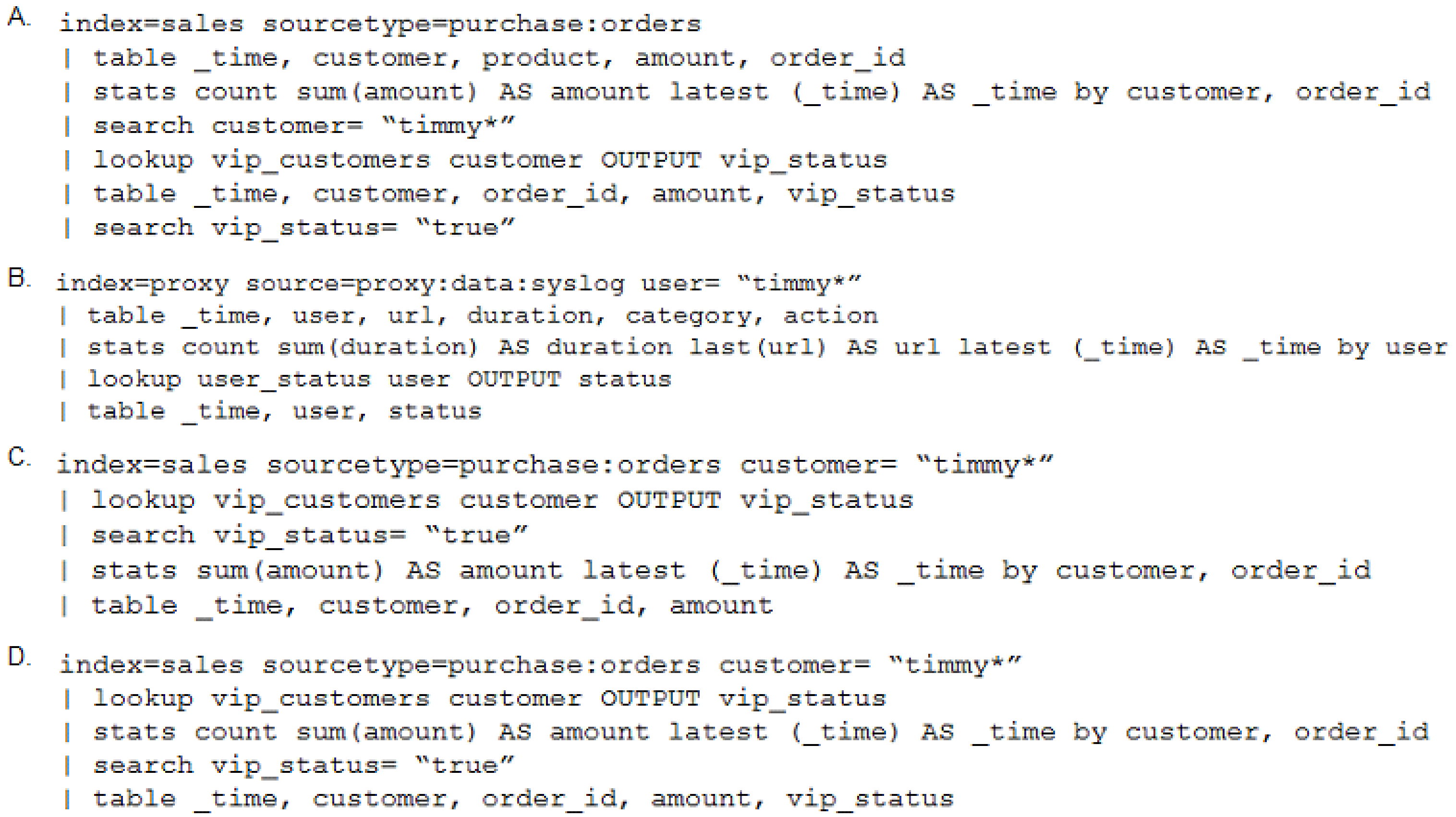
Question Type: **MultipleChoice**

A customer has written the following search:



```
sourcetype=purchase:orders
| table _time, customer, product, amount, order_id
| stats count sum(amount) AS amount latest (_time) AS _time by customer, order_id
| search customer= “timmy*”
| lookup vip_customers customer OUTPUT vip_status
| table _time, customer, order_id, amount, vip_status
| search vip_status= “true”
```

How can the search be rewritten to maximize efficiency?



A.
```
index=sales sourcetype=purchase:orders
| table _time, customer, product, amount, order_id
| stats count sum(amount) AS amount latest (_time) AS _time by customer, order_id
| search customer= “timmy*”
| lookup vip_customers customer OUTPUT vip_status
| table _time, customer, order_id, amount, vip_status
| search vip_status= “true”
```

B.
```
index=proxy source=proxy:data:syslog user= “timmy*”
| table _time, user, url, duration, category, action
| stats count sum(duration) AS duration last(url) AS url latest (_time) AS _time by user
| lookup user_status user OUTPUT status
| table _time, user, status
```

C.
```
index=sales sourcetype=purchase:orders customer= “timmy*”
| lookup vip_customers customer OUTPUT vip_status
| search vip_status= “true”
| stats sum(amount) AS amount latest (_time) AS _time by customer, order_id
| table _time, customer, order_id, amount
```

D.
```
index=sales sourcetype=purchase:orders customer= “timmy*”
| lookup vip_customers customer OUTPUT vip_status
| stats count sum(amount) AS amount latest (_time) AS _time by customer, order_id
| search vip_status= “true”
| table _time, customer, order_id, amount, vip_status
```

Options:

A- Option A

B- Option B

C- Option C

D- Option D

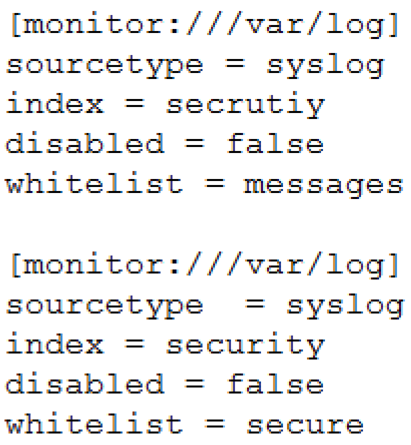
Answer:

C

Question 4

Question Type: MultipleChoice

Consider the scenario where the /var/log directory contains the files secure, messages, cron, audit. A customer has created the following inputs.conf stanzas in the same Splunk app in order to attempt to monitor the files secure and messages:



```
[monitor:///var/log]
sourcetype = syslog
index = secrutiy
disabled = false
whitelist = messages

[monitor:///var/log]
sourcetype  = syslog
index = security
disabled = false
whitelist = secure
```

Which file(s) will actually be actively monitored?

Options:

A- /var/log/secure

B- /var/log/messages

C- /var/log/messages, /var/log/cron, /var/log/audit, /var/log/secure

D- /var/log/secure, /var/log/messages

Answer:

A

Question 5

Question Type: **MultipleChoice**

The customer wants to migrate their current Splunk Index cluster to new hardware to improve indexing and search performance. What is the correct process and procedure for this task?

Options:

A- 1. Install new indexers.

2. Configure indexers into the cluster as peers; ensure they receive the same configuration via the deployment server.

3. Decommission old peers one at a time.

4. Remove old peers from the CM's list.

5. Update forwarders to forward to the new peers.

B- 1. Install new indexers.

2. Configure indexers into the cluster as peers; ensure they receive the cluster bundle and the same configuration as original peers.

3. Decommission old peers one at a time.

4. Remove old peers from the CM's list.

5. Update forwarders to forward to the new peers.

C- 1. Install new indexers.

2. Configure indexers into the cluster as peers; ensure they receive the same configuration via the deployment server.

3. Update forwarders to forward to the new peers.

4. Decommission old peers on at a time.

5. Restart the cluster master (CM).

D- 1. Install new indexers.

2. Configure indexers into the cluster as peers; ensure they receive the cluster bundle and the same configuration as original peers.

3. Update forwarders to forward to the new peers.

4. Decommission old peers one at a time.

5. Remove old peers from the CM's list.

Answer:

C

Question 6

Question Type: **MultipleChoice**

A customer has a Universal Forwarder (UF) with an inputs.conf monitoring its splunkd.log. The data is sent through a heavy forwarder to an indexer. Where does the Index time parsing occur?

Options:

A- Indexer

B- Universal forwarder

C- Search head

D- Heavy forwarder

Answer:

D

Question 7

Question Type: MultipleChoice

An index receives approximately 50GB of data per day per indexer at an even and consistent rate. The customer would like to keep this data searchable for a minimum of 30 days. In addition, they have hourly scheduled searches that process a week's worth of data and are quite sensitive to search performance.

Given ideal conditions (no restarts, nor drops/bursts in data volume), and following PS best practices, which of the following sets of indexes.conf settings can be leveraged to meet the requirements?

Options:

A- frozenTimePeriodInSecs, maxDataSize, maxVolumeDataSizeMB, maxHotBuckets

B- maxDataSize, maxTotalDataSizeMB, maxHotBuckets, maxGlobalDataSizeMB

C- maxDataSize, frozenTimePeriodInSecs, maxVolumeDataSizeMB

D- frozenTimePeriodInSecs, maxWarmDBCount, homePath.maxDataSizeMB, maxHotSpanSecs

Answer:

B