SPLK-3003 Q&As

Splunk Core Certified Consultant

Pass Splunk SPLK-3003 Exam with 100% Guarantee

Free Download Real Questions & Answers **PDF** and **VCE** file from:

https://www.passapply.com/splk-3003.html

100% Passing Guarantee
100% Money Back Assurance

Following Questions and Answers are all new published by Splunk Official Exam Center

- **Instant Download** After Purchase
- **100% Money Back** Guarantee
- **365 Days** Free Update
- **800,000+** Satisfied Customers

QUESTION 1

A customer is using both internal Splunk authentication and LDAP for user management.

If a username exists in both $SPLUNK_HOME/etc/passwd and LDAP, which of the following statements is

accurate?

A. The internal Splunk authentication will take precedence.

B. Authentication will only succeed if the password is the same in both systems.

C. The LDAP user account will take precedence.

D. Splunk will error as it does not support overlapping usernames

Correct Answer: A

QUESTION 2

Report acceleration has been enabled for a specific use case. In which bucket location is the corresponding CSV file located?

A. thawedPath

B. summaryHomePath

C. tstatsHomePath

D. homePath, coldPath

Correct Answer: B

Reference: https://docs.splunk.com/Documentation/Splunk/8.1.0/Knowledge/ Manageacceleratedsearchsummaries

QUESTION 3

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

A. Deployer sharing with master cluster.

B. License master that has 50 clients or more.

C. Cluster master node

D. Production Search Head

Correct Answer: C

Reference: https://docs.splunk.com/Documentation/Splunk/8.1.0/DMC/WheretohostDMC

QUESTION 4

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
```

A. Option A

B. Option B

C. Option C

D. Option D

Correct Answer: C

QUESTION 5

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

A. When joining results from multiple indexes.

B. When dynamically filtering hosts.

C. When filtering indexed fields.

D. When joining multiple large datasets.

Correct Answer: A