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.pass4itsure.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

The data in Splunk is now subject to auditing and compliance controls. A customer would like to ensure that at least one year of logs are retained for both Windows and Firewall events. What data retention controls must be configured?

A. maxTotalDataSizeMB and frozenTimePeriodInSecs

B. coldToFrozenDir and coldToFrozenScript

C. Splunk Volume and maxTotalDataSizMB

D. Splunk Volume and frozenTimePeriodInSecs

Correct Answer: A

Reference: https://docs.splunk.com/Documentation/Splunk/8.1.0/Indexer/Setaretirementandarchivingpolicy

QUESTION 2

What happens to the indexer cluster when the indexer Cluster Master (CM) runs out of disk space?

A. A warm standby CM needs to be brought online as soon as possible before an indexer has an outage.

B. The indexer cluster will continue to operate as long as no indexers fail.

C. If the indexer cluster has site failover configured in the CM, the second cluster master will take over.

D. The indexer cluster will continue to operate as long as a replacement CM is deployed within 24 hours.

Correct Answer: C

QUESTION 3

What is the default push mode for a search head cluster deployer app configuration bundle?

A. full

B. merge_to_default

C. default_only

D. local_only

Correct Answer: B

Reference: https://docs.splunk.com/Documentation/Splunk/8.1.0/DistSearch/PropagateSHCconfigurationchanges#:~:text=The%20deployer%20push%20mode%20determines,default%20push%20mode%20is%20merge_to_default%20

QUESTION 4

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

A. AUTO_KV_JSON

B. BREAK_ONLY_BEFORE_DATE

C. SHOULD_LINEMERGE

D. ANNOTATE_PUNCT

Correct Answer: C

Reference: https://docs.splunk.com/Documentation/Splunk/8.0.6/Data/Configureeventlinebreaking

QUESTION 5

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