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.geekcert.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 has a network device that transmits logs directly with UDP or TCP over SSL. Using PS best practices, which ingestion method should be used?

A. Open a TCP port with SSL on a heavy forwarder to parse and transmit the data to the indexing tier.

B. Open a UDP port on a universal forwarder to parse and transmit the data to the indexing tier.

C. Use a syslog server to aggregate the data to files and use a heavy forwarder to read and transmit the data to the indexing tier.

D. Use a syslog server to aggregate the data to files and use a universal forwarder to read and transmit the data to the indexing tier.

Correct Answer: D

QUESTION 2

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?

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.

Correct Answer: A

QUESTION 3

A customer has implemented their own Role Based Access Control (RBAC) model to attempt to give the Security team different data access than the Operations team by creating two new Splunk roles ?security and operations. In the srchIndexesAllowed setting of authorize.conf, they specified the network index under the security role and the operations index under the operations role. The new roles are set up to inherit the default user role.

If a new user is created and assigned to the operations role only, which indexes will the user have access to search?

A. operations, network, _internal, _audit

B. operations

C. No Indexes

D. operations, network

Correct Answer: A

QUESTION 4

Which of the following is the most efficient search?

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

Correct Answer: B

QUESTION 5

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

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.

Correct Answer: B

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