Vendor: Splunk

Exam Code:SPLK-3003

Exam Name: Splunk Core Certified Consultant

Version: Demo

QUESTION 1

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 2

What should be considered when running the following CLI commands with a goal of accelerating an index cluster migration to new hardware?

```
$SPLUNK_HOME/bin/splunk edit cluster-config -max_peer_build_load 3

$SPLUNK_HOME/bin/splunk edit cluster-config -max_peer_rep_load 6
```

server.conf

```
[clustering]

max_peer_build_load = 2

max_peer_rep_load = 5
```

A. Data ingestion rate

B. Network latency and storage IOPS

C. Distance and location

D. SSL data encryption

Correct Answer: B

QUESTION 3

A working search head cluster has been set up and used for 6 months with just the native/local Splunk user authentication method. In order to integrate the search heads with an external Active Directory server using LDAP, which of the following statements represents the most appropriate method to deploy the configuration to the servers?

A. Configure the integration in a base configuration app located in shcluster-apps directory on the search head deployer, then deploy the configuration to the search heads using the splunk apply shclusterbundle command.

B. Log onto each search using a command line utility. Modify the authentication.conf and authorize.conf files in a base configuration app to configure the integration.

C. Configure the LDAP integration on one Search Head using the Settings > Access Controls > Authentication Method and Settings > Access Controls > Roles Splunk UI menus. The configuration setting will replicate to the other nodes in the search head cluster eliminating the need to do this on the other search heads.

D. On each search head, login and configure the LDAP integration using the Settings > Access Controls > Authentication Method and Settings > Access Controls > Roles Splunk UI menus.

Correct Answer: C

Reference: https://docs.splunk.com/Documentation/Splunk/8.1.0/Security/ConfigureLDAPwithSplunkWeb

---

QUESTION 4

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

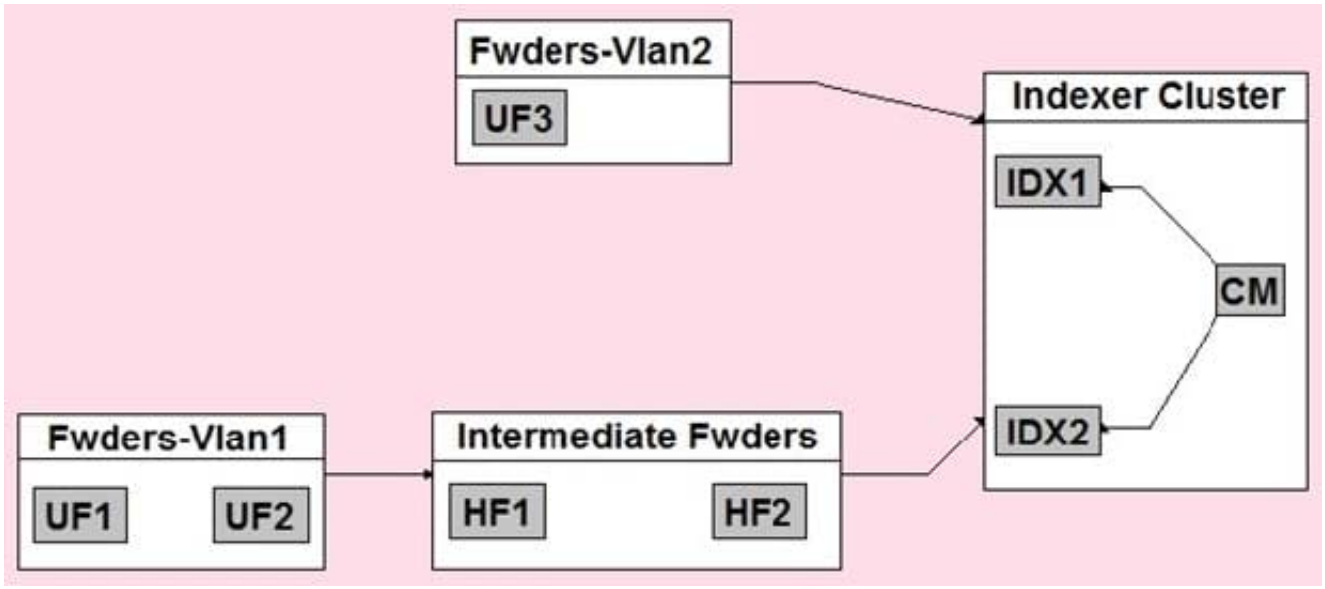
Correct Answer: B

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

---

QUESTION 5

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?



A. All universal forwarders.

B. Only the indexers.

C. All heavy forwarders.

D. On all parsing Splunk instances.

Correct Answer: D

QUESTION 6

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

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.

Correct Answer: B

QUESTION 7

What happens when an index cluster peer freezes a bucket?

A. All indexers with a copy of the bucket will delete it.

B. The cluster master will ensure another copy of the bucket is made on the other peers to meet the replication settings.

C. The cluster master will no longer perform fix-up activities for the bucket.

D. All indexers with a copy of the bucket will immediately roll it to frozen.

Correct Answer: C

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

---

QUESTION 8

A new single-site three indexer cluster is being stood up with replication_factor:2, search_factor:2. At which step would the Indexer Cluster be classed as `Indexing Ready\\' and be able to ingest new data?

Step 1: Install and configure Cluster Master (CM)/Master Node with base clustering stanza settings, restarting CM.

Step 2: Configure a base app in etc/master-apps on the CM to enable a splunktcp input on port 9997 and deploy index creation configurations.

Step 3: Install and configure Indexer 1 so that once restarted, it contacts the CM, download the latest config bundle.

Step 4: Indexer 1 restarts and has successfully joined the cluster.

Step 5: Install and configure Indexer 2 so that once restarted, it contacts the CM, downloads the latest config bundle

Step 6: Indexer 2 restarts and has successfully joined the cluster.

Step 7: Install and configure Indexer 3 so that once restarted, it contacts the CM, downloads the latest config bundle.

Step 8: Indexer 3 restarts and has successfully joined the cluster.

A. Step 2

B. Step 4

C. Step 6

D. Step 8

Correct Answer: A

QUESTION 9

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 10

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 11

Which statement is true about subsearches?

A. Subsearches are faster than other types of searches.

B. Subsearches work best for joining two large result sets.

C. Subsearches run at the same time as their outer search.

D. Subsearches work best for small result sets.

Correct Answer: A

Reference: https://community.splunk.com/t5/Archive/Looking-for-way-to-explain-why-subsearches-are-soslow/m-p/479133

QUESTION 12

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