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 migrating their existing Splunk Indexer from an old set of hardware to a new set of indexers. What is the earliest method to migrate the system?

A. 1. Add new indexers to the cluster as peers, in the same site (if needed).

2.

Ensure new indexers receive common configuration.

3.

Decommission old indexers (one at a time) to allow time for CM to fix/migrate buckets to new

hardware.

4.

Remove all the old indexers from the CM\\'s list.

B. 1. Add new indexers to the cluster as peers, to a new site.

2.

Ensure new indexers receive common configuration from the CM.

3.

Decommission old indexers (one at a time) to allow time for CM to fix/migrate buckets to new

hardware.

4.

Remove all the old indexers from the CM\\'s list.

C. 1. Add new indexers to the cluster as peers, in the same site.

2.

Update the replication factor by +1 to Instruct the cluster to start replicating to new peers.

3.

Allow time for CM to fix/migrate buckets to new hardware.

4.

Remove all the old indexers from the CM\\'s list.

D. 1. Add new indexers to the cluster as new site.

2.

Update cluster master (CM) server.conf to include the new available site.

3.

Allow time for CM to fix/migrate buckets to new hardware.

4.

Remove the old indexers from the CM\\'s list.

Correct Answer: B

QUESTION 2

Which of the following statements applies to indexer discovery?

A. The Cluster Master (CM) can automatically discover new indexers added to the cluster.

B. Forwarders can automatically discover new indexers added to the cluster.

C. Deployment servers can automatically configure new indexers added to the cluster.

D. Search heads can automatically discover new indexers added to the cluster.

Correct Answer: D

Reference: https://docs.splunk.com/Documentation/Splunk/8.1.0/DistSearch/Connectclustersearchheadstosearchpeers

QUESTION 3

As a best practice which of the following should be used to ingest data on clustered indexers?

A. Monitoring (via a process), collecting data (modular inputs) from remote systems/applications

B. Modular inputs, HTTP Event Collector (HEC), inputs.conf monitor stanza

C. Actively listening on ports, monitoring (via a process), collecting data from remote systems/applications

D. splunktcp, splunktcp-ssl, HTTP Event Collector (HEC)

Correct Answer: B

QUESTION 4

A customer wants to implement LDAP because managing local Splunk users is becoming too much of an overhead. What configuration details are needed from the customer to implement LDAP authentication?

A. API: Python script with PAM/RADIUS details.

B. LDAP server: port, bind user credentials, path/to/groups, path/to/user.

C. LDAP server: port, bind user credentials, base DN for groups, base DN for users.

D. LDAP REST details, base DN for groups, base DN for users.

Correct Answer: C

Reference: https://www.learnsplunk.com/splunk-ldap-authentication-configuration.html

QUESTION 5

Consider the search shown below.

```
index=web sourcetype=web_log [ search index=firewall action=denied
severity=high | stats latest (_time) as _time | eval
earliest=tostring(relative_time (_time, "-2h@h")), latest=tostring
(relative_time(_time, "+2h@h")) | fields earliest, latest]
```

What is this search\\'s intended function?

A. To return all the web_log events from the web index that occur two hours before and after the most recent high severity, denied event found in the firewall index.

B. To find all the denied, high severity events in the firewall index, and use those events to further search for lateral movement within the web index.

C. To return all the web_log events from the web index that occur two hours before and after all high severity, denied events found in the firewall index.

D. To search the firewall index for web logs that have been denied and are of high severity.

Correct Answer: C