SPLK-2002$^{Q\&As}$

Splunk Enterprise Certified Architect

Pass Splunk SPLK-2002 Exam with 100% Guarantee

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

QUESTION 1

When adding or decommissioning a member from a Search Head Cluster (SHC), what is the proper order of operations?

A. 1. Delete Splunk Enterprise, if it exists.

2.

Install and initialize the instance.

3.

Join the SHC.

B. 1. Install and initialize the instance.

2.

Delete Splunk Enterprise, if it exists.

3.

Join the SHC.

C. 1. Initialize cluster rebalance operation.

2.

Remove master node from cluster.

3.

Trigger replication.

D. 1. Trigger replication.

2.

Remove master node from cluster.

3.

Initialize cluster rebalance operation.

Correct Answer: B

QUESTION 2

Which of the following statements describe search head clustering? (Select all that apply.)

A. A deployer is required.

B. At least three search heads are needed.

C. Search heads must meet the high-performance reference server requirements.

D. The deployer must have sufficient CPU and network resources to process service requests and push configurations.

Correct Answer: AC

QUESTION 3

In an existing Splunk environment, the new index buckets that are created each day are about half the size of the incoming data. Within each bucket, about 30% of the space is used for rawdata and about 70% for index files.

What additional information is needed to calculate the daily disk consumption, per indexer, if indexer clustering is implemented?

A. Total daily indexing volume, number of peer nodes, and number of accelerated searches.

B. Total daily indexing volume, number of peer nodes, replication factor, and search factor.

C. Total daily indexing volume, replication factor, search factor, and number of search heads.

D. Replication factor, search factor, number of accelerated searches, and total disk size across cluster.

Correct Answer: D

QUESTION 4

When Splunk is installed, where are the internal indexes stored by default?

A. SPLUNK_HOME/bin

B. SPLUNK_HOME/var/lib

C. SPLUNK_HOME/var/run

D. SPLUNK_HOME/etc/system/default

Correct Answer: B

Reference: https://answers.splunk.com/answers/3806/where-does-splunk-store-the-logs.html

QUESTION 5

When adding or rejoining a member to a search head cluster, the following error is displayed: Error pulling configurations from the search head cluster captain; consider performing a destructive configuration resync on this search head cluster member.

What corrective action should be taken?

A. Restart the search head.

B. Run the splunk apply shcluster-bundle command from the deployer.

C. Run the clean raft command on all members of the search head cluster.

D. Run the splunk resync shcluster-replicated-config command on this member.

Correct Answer: B

QUESTION 6

What does setting site=site0 on all Search Head Cluster members do in a multi-site indexer cluster?

A. Disables search site affinity.

B. Sets all members to dynamic captaincy.

C. Enables multisite search artifact replication.

D. Enables automatic search site affinity discovery.

Correct Answer: A

Reference: https://docs.splunk.com/Documentation/Splunk/7.3.2/DistSearch/DeploymultisiteSHC

QUESTION 7

Which of the following statements about integrating with third-party systems is true? (Select all that apply.)

A. A Hadoop application can search data in Splunk.

B. Splunk can search data in the Hadoop File System (HDFS).

C. You can use Splunk alerts to provision actions on a third-party system.

D. You can forward data from Splunk forwarder to a third-party system without indexing it first.

Correct Answer: CD

QUESTION 8

What log file would you search to verify if you suspect there is a problem interpreting a regular expression in a monitor stanza?

A. btool.log

B. metrics.log

C. splunkd.log

D. tailing_processor.log

Correct Answer: C

Reference: https://answers.splunk.com/answers/479312/how-to-edit-inputsconf-to-monitor-multiple-files-w

1.html

QUESTION 9

Which command will permanently decommission a peer node operating in an indexer cluster?

A. splunk stop -f

B. splunk offline -f

C. splunk offline --enforce-counts

D. splunk decommission --enforce counts

Correct Answer: C

Reference: https://docs.splunk.com/Documentation/Splunk/7.3.2/Indexer/Takeapeeroffline

QUESTION 10

As a best practice, where should the internal licensing logs be stored?

A. Indexing layer.

B. License server.

C. Deployment layer.

D. Search head layer.

Correct Answer: D

Reference: https://docs.splunk.com/Documentation/ITSI/4.3.1/Install/Plan

QUESTION 11

What is the minimum reference server specification for a Splunk indexer?

A. 12 CPU cores, 12GB RAM, 800 IOPS

B. 16 CPU cores, 16GB RAM, 800 IOPS

C. 24 CPU cores, 16GB RAM, 1200 IOPS

D. 28 CPU cores, 32GB RAM, 1200 IOPS

Correct Answer: A

Reference: https://docs.splunk.com/Documentation/Splunk/7.3.2/Capacity/
Referencehardware#Reference_host_specification

QUESTION 12

Which of the following should be done when installing Enterprise Security on a Search Head Cluster? (Select all that apply.)

A. Install Enterprise Security on the deployer.

B. Install Enterprise Security on a staging instance.

C. Copy the Enterprise Security configurations to the deployer.

D. Use the deployer to deploy Enterprise Security to the cluster members.

Correct Answer: AD

Reference: https://docs.splunk.com/Documentation/ES/5.3.1/Install/InstallEnterpriseSecuritySHC

QUESTION 13

The guidance Splunk gives for estimating size on for syslog data is 50% of original data size. How does this divide between files in the index?

A. rawdata is: 10%, tsidx is: 40%

B. rawdata is: 15%, tsidx is: 35%

C. rawdata is: 35%, tsidx is: 15%

D. rawdata is: 40%, tsidx is: 10%

Correct Answer: B

Reference: https://answers.splunk.com/answers/147951/what-is-the-compression-ratio-of-raw-data-insplunk.html

QUESTION 14

Which Splunk Enterprise offering has its own license?

A. Splunk Cloud Forwarder

B. Splunk Heavy Forwarder

C. Splunk Universal Forwarder

D. Splunk Forwarder Management

Correct Answer: C

Reference: https://docs.splunk.com/Splexicon:Forwardinglicense

QUESTION 15

Which tool(s) can be leveraged to diagnose connection problems between an indexer and forwarder? (Select all that apply.)

A. telnet

B. tcpdump

C. splunk btool

D. splunk btprobe

Correct Answer: BC

Reference: https://docs.splunk.com/Documentation/Splunk/7.3.2/Security/
Troubleshootyouforwardertoindexerauthentication