Splunk Enterprise Certified Architect Exam

Splunk SPLK-2002

Version Demo

Total Demo Questions: 10

Total Premium Questions: 90

Buy Premium PDF

QUESTION NO: 1

Consider a use case involving firewall data. There is no Splunk-supported Technical Add-On, but the vendor has built one. What are the items that must be evaluated before installing the add-on? (Select all that apply.)

A. Identify number of scheduled or real-time searches.

B. Validate if this Technical Add-On enables event data for a data model.

C. Identify the maximum number of forwarders Technical Add-On can support.

D. Verify if Technical Add-On needs to be installed onto both a search head or indexer.

ANSWER: A C

QUESTION NO: 2

Which command is used for thawing the archive bucket?

A. Splunk collect

B. Splunk convert

C. Splunk rebuild

D. Splunk dbinspect

ANSWER: C

Explanation:

Reference: https://answers.splunk.com/answers/337025/after-frozen-data-restore-thawed-data-not-working.html

QUESTION NO: 3

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.

ANSWER: C D

QUESTION NO: 4

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.

ANSWER: A D

Explanation:

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

QUESTION NO: 5

Indexing is slow and real-time search results are delayed in a Splunk environment with two indexers and one search head. There is ample CPU and memory available on the indexers. Which of the following is most likely to improve indexing performance?

A. Increase the maximum number of hot buckets in indexes.conf

B. Increase the number of parallel ingestion pipelines in server.conf

C. Decrease the maximum size of the search pipelines in limits.conf

D. Decrease the maximum concurrent scheduled searches in limits.conf

ANSWER: D

QUESTION NO: 6

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.

ANSWER: D

QUESTION NO: 7

A multi-site indexer cluster can be configured using which of the following? (Select all that apply.)

A. Via Splunk Web.

B. Directly edit SPLUNK_HOME/etc/system/local/server.conf

C. Run a splunk edit cluster-config command from the CLI.

D. Directly edit SPLUNK_HOME/etc/system/default/server.conf

ANSWER: A B

Explanation:

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

QUESTION NO: 8

When planning a search head cluster, which of the following is true?

A. All search heads must use the same operating system.

B. All search heads must be members of the cluster (no standalone search heads).

C. The search head captain must be assigned to the largest search head in the cluster.

D. All indexers must belong to the underlying indexer cluster (no standalone indexers).

ANSWER: C

QUESTION NO: 9

When converting from a single-site to a multi-site cluster, what happens to existing single-site clustered buckets?

A. They will continue to replicate within the origin site and age out based on existing policies.

B. They will maintain replication as required according to the single-site policies, but never age out.

C. They will be replicated across all peers in the multi-site cluster and age out based on existing policies.

D. They will stop replicating within the single-site and remain on the indexer they reside on and age out according to existing policies.

ANSWER: B

Explanation:

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

QUESTION NO: 10

Which of the following artifacts are included in a Splunk diag file? (Select all that apply.)

A. OS settings.

B. Internal logs.

C. Customer data.

D. Configuration files.

ANSWER: B D

Explanation:

Reference: https://docs.splunk.com/Documentation/Splunk/7.3.2/Troubleshooting/Generateadiag