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

What is the logical first step when starting a deployment plan?

A. Inventory the currently deployed logging infrastructure.

B. Determine what apps and use cases will be implemented.

C. Gather statistics on the expected adoption of Splunk for sizing.

D. Collect the initial requirements for the deployment from all stakeholders.

Correct Answer: D

QUESTION 2

Which of the following security options must be explicitly configured (i.e. which options are not enabled by default)?

A. Data encryption between Splunk Web and splunkd.

B. Certificate authentication between forwarders and indexers.

C. Certificate authentication between Splunk Web and search head.

D. Data encryption for distributed search between search heads and indexers.

Correct Answer: B

QUESTION 3

Which Splunk internal index contains license-related events?

A. _audit

B. _license

C. _internal

D. _introspection

Correct Answer: C

Reference: https://answers.splunk.com/answers/579494/how-to-display-license-consumed-by-an-indexover-2.html

QUESTION 4

Which of the following is true regarding Splunk Enterprise performance? (Select all that apply.)

A. Adding search peers increases the maximum size of search results.

B. Adding RAM to an existing search heads provides additional search capacity.

C. Adding search peers increases the search throughput as search load increases.

D. Adding search heads provides additional CPU cores to run more concurrent searches.

Correct Answer: BD

Reference: https://docs.splunk.com/Documentation/Splunk/7.3.2/Capacity/HowsavedsearchesaffectSplunkEnterpriseperformance

QUESTION 5

The frequency in which a deployment client contacts the deployment server is controlled by what?

A. polling_interval attribute in outputs.conf

B. phoneHomeIntervalInSecs attribute in outputs.conf

C. polling_interval attribute in deploymentclient.conf

D. phoneHomeIntervalInSecs attribute in deploymentclient.conf

Correct Answer: D

Reference: https://docs.splunk.com/Documentation/SplunkCloud/7.2.7/RESTREF/RESTdeploy

QUESTION 6

Which CLI command converts a Splunk instance to a license slave?

A. splunk add licenses

B. splunk list licenser-slaves

C. splunk edit licenser-localslave

D. splunk list licenser-localslave

Correct Answer: C

Reference: https://docs.splunk.com/Documentation/Splunk/7.3.2/Admin/LicenserCLIcommands

QUESTION 7

Which Splunk server role regulates the functioning of indexer cluster?

A. Indexer

B. Deployer

C. Master Node

D. Monitoring Console

Correct Answer: C

Reference: https://docs.splunk.com/Documentation/Splunk/7.3.1/Deploy/Indexercluster

QUESTION 8

Which index-time props.conf attributes impact indexing performance? (Select all that apply.)

A. REPORT

B. LINE_BREAKER

C. ANNOTATE_PUNCT

D. SHOULD_LINEMERGE

Correct Answer: BD

Reference: https://docs.splunk.com/Documentation/Splunk/7.3.2/Data/Configureeventlinebreaking

QUESTION 9

Search dashboards in the Monitoring Console indicate that the distributed deployment is approaching its capacity. Which of the following options will provide the most search performance improvement?

A. Replace the indexer storage to solid state drives (SSD).

B. Add more search heads and redistribute users based on the search type.

C. Look for slow searches and reschedule them to run during an off-peak time.

D. Add more search peers and make sure forwarders distribute data evenly across all indexers.

Correct Answer: C

QUESTION 10

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 11

Which command is used for thawing the archive bucket?

A. Splunk collect

B. Splunk convert

C. Splunk rebuild

D. Splunk dbinspect

Correct Answer: C

Reference: https://answers.splunk.com/answers/337025/after-frozen-data-restore-thawed-data-notworking.html

QUESTION 12

Because Splunk indexing is read/write intensive, it is important to select the appropriate disk storage solution for each deployment. Which of the following statements is accurate about disk storage?

A. High performance SAN should never be used.

B. Enable NFS for storing hot and warm buckets.

C. The recommended RAID setup is RAID 10 (1 + 0).

D. Virtualized environments are usually preferred over bare metal for Splunk indexers.

Correct Answer: C

Reference: https://www.splunk.com/pdfs/technical-briefs/splunk-deploying-vmware-tech-brief.pdf

QUESTION 13

When should multiple search pipelines be enabled?

A. Only if disk IOPS is at 800 or better.

B. Only if there are fewer than twelve concurrent users.

C. Only if running Splunk Enterprise version 6.6 or later.

D. Only if CPU and memory resources are significantly under-utilized.

Correct Answer: D

Reference: https://answers.splunk.com/answers/617608/can-we-increase-parallelingestionpipelines-in-ahe.html

QUESTION 14

A customer has installed a 500GB Enterprise license. They also purchased and installed a 300GB, no enforcement license on the same license master. How much data can the customer ingest before search is locked out?

A. 300GB. After this limit, search is locked out.

B. 500GB. After this limit, search is locked out.

C. 800GB. After this limit, search is locked out.

D. Search is not locked out. Violations are still recorded.

Correct Answer: D

Reference: https://docs.splunk.com/Documentation/Splunk/7.3.2/Admin/TypesofSplunklicenses

QUESTION 15

In the deployment planning process, when should a person identify who gets to see network data?

A. Deployment schedule

B. Topology diagramming

C. Data source inventory

D. Data policy definition

Correct Answer: C