

Exam Questions SPLK-2002

Splunk Enterprise Certified Architect

<https://www.2passeasy.com/dumps/SPLK-2002/>



NEW QUESTION 1

Which of the following will cause the greatest reduction in disk size requirements for a cluster of N indexers running Splunk Enterprise Security?

- A. Setting the cluster search factor to N-1.
- B. Increasing the number of buckets per index.
- C. Decreasing the data model acceleration range.
- D. Setting the cluster replication factor to N-1.

Answer: D

NEW QUESTION 2

Stakeholders have identified high availability for searchable data as their top priority. Which of the following best addresses this requirement?

- A. Increasing the search factor in the cluster.
- B. Increasing the replication factor in the cluster.
- C. Increasing the number of search heads in the cluster.
- D. Increasing the number of CPUs on the indexers in the cluster.

Answer: B

NEW QUESTION 3

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.

Answer: C

NEW QUESTION 4

A Splunk architect has inherited the Splunk deployment at Buttercup Games and end users are complaining that the events are inconsistently formatted for a web sourcetype. Further investigation reveals that not all web logs flow through the same infrastructure: some of the data goes through heavy forwarders and some of the forwarders are managed by another department. Which of the following items might be the cause for this issue?

- A. The search head may have different configurations than the indexers.
- B. The data inputs are not properly configured across all the forwarders.
- C. The indexers may have different configurations than the heavy forwarders.
- D. The forwarders managed by the other department are an older version than the rest.

Answer: D

NEW QUESTION 5

What does the deployer do in a Search Head Cluster (SHC)? (Select all that apply.)

- A. Distributes apps to SHC members.
- B. Bootstraps a clean Splunk install for a SHC.
- C. Distributes non-search related and manual configuration file changes.
- D. Distributes runtime knowledge object changes made by users across the SHC.

Answer: A

NEW QUESTION 6

When using the props.conf LINE_BREAKER attribute to delimit multi-line events, the SHOULD_LINEMERGE attribute should be set to what?

- A. Auto
- B. None
- C. True
- D. False

Answer: C

NEW QUESTION 7

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

- A. REPORT
- B. LINE_BREAKER
- C. ANNOTATE_PUNCT
- D. SHOULD_LINEMERGE

Answer: BD

NEW QUESTION 8

Which of the following are client filters available in serverclass.conf? (Select all that apply.)

- A. DNS name.
- B. IP address.
- C. Splunk server role.
- D. Platform (machine type).

Answer: AB

NEW QUESTION 9

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

Answer: C

NEW QUESTION 10

Which Splunk tool offers a health check for administrators to evaluate the health of their Splunk deployment?

- A. btool
- B. DiagGen
- C. SPL Clinic
- D. Monitoring Console

Answer: D

NEW QUESTION 10

In a four site indexer cluster, which configuration stores two searchable copies at the origin site, one searchable copy at site2, and a total of four searchable copies?

- A. site_search_factor = origin:2, site1:2, total:4
- B. site_search_factor = origin:2, site2:1, total:4
- C. site_replication_factor = origin:2, site1:2, total:4
- D. site_replication_factor = origin:2, site2:1, total:4

Answer: D

NEW QUESTION 12

Which Splunk Enterprise offering has its own license?

- A. Splunk Cloud Forwarder
- B. Splunk Heavy Forwarder
- C. Splunk Universal Forwarder
- D. Splunk Forwarder Management

Answer: C

NEW QUESTION 13

Which Splunk server role regulates the functioning of indexer cluster?

- A. Indexer
- B. Deployer
- C. Master Node
- D. Monitoring Console

Answer: C

NEW QUESTION 14

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.

Answer: B

NEW QUESTION 17

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%

Answer: B

NEW QUESTION 20

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

NEW QUESTION 24

To activate replication for an index in an indexer cluster, what attribute must be configured in indexes.conf on all peer nodes?

- A. repFactor = 0
- B. replicate = 0
- C. repFactor = auto
- D. replicate = auto

Answer: C

NEW QUESTION 25

Which of the following clarification steps should be taken if apps are not appearing on a deployment client? (Select all that apply.)

- A. Check serverclass.conf of the deployment server.
- B. Check deploymentclient.conf of the deployment client.
- C. Check the content of SPLUNK_HOME/etc/apps of the deployment server.
- D. Search for relevant events in splunkd.log of the deployment server.

Answer: ABC

NEW QUESTION 30

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.

Answer: B

NEW QUESTION 34

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

Answer: C

NEW QUESTION 39

Which of the following can a Splunk diag contain?

- A. Search history, Splunk users and their roles, running processes, indexed data
- B. Server specs, current open connections, internal Splunk log files, index listings
- C. KV store listings, internal Splunk log files, search peer bundles listings, indexed data
- D. Splunk platform configuration details, Splunk users and their roles, current open connections, index listings

Answer: B

NEW QUESTION 40

A customer plans to ingest 600 GB of data per day into Splunk. They will have six concurrent users, and they also want high data availability and high search

performance. The customer is concerned about cost and wants to spend the minimum amount on the hardware for Splunk. How many indexers are recommended for this deployment?

- A. Two indexers not in a cluster, assuming users run many long searches.
- B. Three indexers not in a cluster, assuming a long data retention period.
- C. Two indexers clustered, assuming high availability is the greatest priority.
- D. Two indexers clustered, assuming a high volume of saved/scheduled searches.

Answer: D

NEW QUESTION 42

At which default interval does metrics.log generate a periodic report regarding license utilization?

- A. 10 seconds
- B. 30 seconds
- C. 60 seconds
- D. 300 seconds

Answer: B

NEW QUESTION 43

Which of the following is a good practice for a search head cluster deployer?

- A. The deployer only distributes configurations to search head cluster members when they “phone home”.
- B. The deployer must be used to distribute non-replicable configurations to search head cluster members.
- C. The deployer must distribute configurations to search head cluster members to be valid configurations.
- D. The deployer only distributes configurations to search head cluster members with splunk apply shcluster-bundle.

Answer: A

NEW QUESTION 48

A new Splunk customer is using syslog to collect data from their network devices on port 514. What is the best practice for ingesting this data into Splunk?

- A. Configure syslog to send the data to multiple Splunk indexers.
- B. Use a Splunk indexer to collect a network input on port 514 directly.
- C. Use a Splunk forwarder to collect the input on port 514 and forward the data.
- D. Configure syslog to write logs and use a Splunk forwarder to collect the logs.

Answer: C

NEW QUESTION 53

When Splunk indexes data in a non clustered environment, what kind of files does it create by default?

- A. Index and .tsidx files.
- B. Rawdata and index files.
- C. Compressed and .tsidx files.
- D. Compressed and meta data files.

Answer: B

NEW QUESTION 56

How does IT Service Intelligence (ITSI) impact the planning of a Splunk deployment?

- A. ITSI requires a dedicated deployment server.
- B. The amount of users using ITSI will not impact performance.
- C. ITSI in a Splunk deployment does not require additional hardware resources.
- D. Depending on the Key Performance Indicators that are being tracked, additional infrastructure may be needed.

Answer: D

NEW QUESTION 59

In search head clustering, which of the following methods can you use to transfer captaincy to a different member? (Select all that apply.)

- A. Use the Monitoring Console.
- B. Use the Search Head Clustering settings menu from Splunk Web on any member.
- C. Run the splunk transfer shcluster-captain command from the current captain.
- D. Run the splunk transfer shcluster-captain command from the member you would like to become the captain.

Answer: BD

NEW QUESTION 62

A Splunk instance has the following settings in SPLUNK_HOME/etc/system/local/server.conf:

```
[clustering] mode = master
replication_factor = 2
pass4SymmKey = password123
```

Which of the following statements describe this Splunk instance? (Select all that apply.)

- A. This is a multi-site cluster.
- B. This cluster's search factor is 2.
- C. This Splunk instance needs to be restarted.
- D. This instance is missing the master_uri attribute.

Answer: AC

NEW QUESTION 66

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.

Answer: A

NEW QUESTION 67

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

NEW QUESTION 70

Which server.conf attribute should be added to the master node's server.conf file when decommissioning a site in an indexer cluster?

- A. site_mappings
- B. available_sites
- C. site_search_factor
- D. site_replication_factor

Answer: A

NEW QUESTION 74

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

Answer: BC

NEW QUESTION 79

A search head has successfully joined a single site indexer cluster. Which command is used to configure the same search head to join another indexer cluster?

- A. splunk add cluster-config
- B. splunk add cluster-master
- C. splunk edit cluster-config
- D. splunk edit cluster-master

Answer: B

NEW QUESTION 82

Which of the following is a best practice to maximize indexing performance?

- A. Use automatic sourcetypes.
- B. Use the Splunk default settings.
- C. Not use pre-trained source types.
- D. Minimize configuration generality.

Answer: D

NEW QUESTION 87

What is the algorithm used to determine captaincy in a Splunk search head cluster?

- A. Raft distributed consensus.

- B. Rapt distributed consensus.
- C. Rift distributed consensus.
- D. Round-robin distribution consensus.

Answer: A

NEW QUESTION 92

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: CD

NEW QUESTION 95

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.

Answer: D

NEW QUESTION 99

In a distributed environment, knowledge object bundles are replicated from the search head to which location on the search peer(s)?

- A. SPLUNK_HOME/var/lib/searchpeers
- B. SPLUNK_HOME/var/log/searchpeers
- C. SPLUNK_HOME/var/run/searchpeers
- D. SPLUNK_HOME/var/spool/searchpeers

Answer: C

NEW QUESTION 100

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: AC

NEW QUESTION 104

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.

Answer: D

NEW QUESTION 106

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.

Answer: AC

NEW QUESTION 110

Which of the following tasks should the architect perform when building a deployment plan? (Select all that apply.)

- A. Use case checklist.
- B. Install Splunk apps.
- C. Inventory data sources.
- D. Review network topology.

Answer: D

NEW QUESTION 114

.....

THANKS FOR TRYING THE DEMO OF OUR PRODUCT

Visit Our Site to Purchase the Full Set of Actual SPLK-2002 Exam Questions With Answers.

We Also Provide Practice Exam Software That Simulates Real Exam Environment And Has Many Self-Assessment Features. Order the SPLK-2002 Product From:

<https://www.2passeasy.com/dumps/SPLK-2002/>

Money Back Guarantee

SPLK-2002 Practice Exam Features:

- * SPLK-2002 Questions and Answers Updated Frequently
- * SPLK-2002 Practice Questions Verified by Expert Senior Certified Staff
- * SPLK-2002 Most Realistic Questions that Guarantee you a Pass on Your FirstTry
- * SPLK-2002 Practice Test Questions in Multiple Choice Formats and Updatesfor 1 Year