Splunk

Exam Questions SPLK-2002

Splunk Enterprise Certified Architect

About Exambible

Your Partner of IT Exam

Found in 1998

Exambible is a company specialized on providing high quality IT exam practice study materials, especially Cisco CCNA, CCDA, CCNP, CCIE, Checkpoint CCSE, CompTIA A+, Network+ certification practice exams and so on. We guarantee that the candidates will not only pass any IT exam at the first attempt but also get profound understanding about the certificates they have got. There are so many alike companies in this industry, however, Exambible has its unique advantages that other companies could not achieve.

Our Advances

* 99.9% Uptime

All examinations will be up to date.

* 24/7 Quality Support

We will provide service round the clock.

* 100% Pass Rate

Our guarantee that you will pass the exam.

* Unique Gurantee

If you do not pass the exam at the first time, we will not only arrange FULL REFUND for you, but also provide you another exam of your claim, ABSOLUTELY FREE!

NEW QUESTION 1
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 2
Which of the following should be included in a deployment plan?

A. Business continuity and disaster recovery plans.
B. Current logging details and data source inventory.
C. Current and future topology diagrams of the IT environment.
D. A comprehensive list of stakeholders, either direct or indirect.

Answer: D

NEW QUESTION 3
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: AB

NEW QUESTION 4
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 5
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 6
A three-node search head cluster is skipping a large number of searches across time. What should be done to increase scheduled search capacity on the search head cluster?

A. Create a job server on the cluster.
B. Add another search head to the cluster.
C. server.conf captain_is_adhoc_searchhead = true.
D. Change limits.conf value for max_searches_per_cpu to a higher value.

Answer: D

NEW QUESTION 7
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 8

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 9
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 10
Which of the following statements describe a Search Head Cluster (SHC) captain? (Select all that apply.)

A. Is the job scheduler for the entire SHC.
B. Manages alert action suppressions (throttling).
C. Synchronizes the member list with the KV store primary.
D. Replicates the SHC's knowledge bundle to the search peers.

Answer: AD

NEW QUESTION 10
Before users can use a KV store, an admin must create a collection. Where is a collection is defined?

A. kvstore.conf
B. collection.conf
C. collections.conf
D. kvcollections.conf

Answer: C

NEW QUESTION 11
Which search will show all deployment client messages from the client (UF)?

A. index=_audit component=DC* host=<ds> | stats count by message
B. index=_audit component=DC* host=<uf> | stats count by message
C. index=_internal component= DC* host=<uf> | stats count by message
D. index=_internal component=DS* host=<ds> | stats count by message

Answer: D

NEW QUESTION 12
To optimize the distribution of primary buckets; when does primary rebalancing automatically occur? (Select all that apply.)

A. Rolling restart completes.
B. Master node rejoins the cluster.
C. Captain joins or rejoins cluster.
D. A peer node joins or rejoins the cluster.

Answer: ABD

NEW QUESTION 15
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 18
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

Answer: C

NEW QUESTION 21
Which of the following describe migration from single-site to multisite index replication?

A. A master node is required at each site.
B. Multisite policies apply to new data only.
C. Single-site buckets instantly receive the multisite policies.
D. Multisite total values should not exceed any single-site factors.

Answer: D

NEW QUESTION 26
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 29
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 31
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 32
Splunk configuration parameter settings can differ between multiple .conf files of the same name contained within different apps. Which of the following directories has the highest precedence?

A. System local directory.
B. System default directory.
C. App local directories, in ASCII order.
D. App default directories, in ASCII order.

Answer: A

NEW QUESTION 35
Which of the following is an indexer clustering requirement?

A. Must use shared storage.
B. Must reside on a dedicated rack.
C. Must have at least three members.
D. Must share the same license pool.

Answer: D

NEW QUESTION 38
How does the average run time of all searches relate to the available CPU cores on the indexers?

A. Average run time is independent of the number of CPU cores on the indexers.
B. Average run time decreases as the number of CPU cores on the indexers decreases.
C. Average run time increases as the number of CPU cores on the indexers decreases.
D. Average run time increases as the number of CPU cores on the indexers increases.

Answer: C

NEW QUESTION 41
When configuring a Splunk indexer cluster, what are the default values for replication and search factor?

A. replication_factor = 2search_factor = 2
B. replication_factor = 2 searchfactor = 3
C. replication_factor = 3search_factor = 2
D. replication_factor = 3 searchfactor = 3

Answer: A

NEW QUESTION 46
Which two sections can be expanded using the Search Job Inspector?

A. Execution costs.
B. Saved search history.
C. Search job properties.
D. Optimization suggestions.

Answer: BC

NEW QUESTION 51
What is a Splunk Job? (Select all that apply.)

A. A user-defined Splunk capability.
B. Searches that are subjected to some usage quota.
C. A search process kicked off via a report or an alert.
D. A child OS process manifested from the splunkd process.

Answer: A

NEW QUESTION 53
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 57
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 58
.....

Relate Links

100% Pass Your SPLK-2002 Exam with Exambible Prep Materials

https://www.exambible.com/SPLK-2002-exam/

Contact us

We are proud of our high-quality customer service, which serves you around the clock 24/7.

Viste - https://www.exambible.com/