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
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 2
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. 300G
B. After this limit, search is locked ou
C. B.500G
D. After this limit, search is locked out.
E. 800G
F. After this limit, search is locked out.
G. Search is not locked ou
H. Violations are still recorded.

Answer: D

NEW QUESTION 3
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 4
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 5
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 6
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.

Answer: BD

NEW QUESTION 7
Which component in the splunkd.log will log information related to bad event breaking?

A. Audittrail
B. EventBreaking
C. IndexingPipeline
D. AggregatorMiningProcessor

Answer: D

NEW QUESTION 8
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

NEW QUESTION 9
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 10
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 10
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

Answer: A

NEW QUESTION 15
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 19
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

Answer: C

NEW QUESTION 24
Splunk Enterprise platform instrumentation refers to data that the Splunk Enterprise deployment logs in the _introspection index. Which of the following logs are included in this index? (Select all that apply.)

A. audit.log
B. metrics.log
C. disk_objects.log
D. resource_usage.log

Answer: CD

NEW QUESTION 27
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 28
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 29
Which search head cluster component is responsible for pushing knowledge bundles to search peers, replicating configuration changes to search head cluster members, and scheduling jobs across the search head cluster?

A. Master
B. Captain
C. Deployer
D. Deployment server

Answer: B

NEW QUESTION 32
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 33
The KV store forms its own cluster within a SHC. What is the maximum number of SHC members KV store will form?

A. 25
B. 50
C. 100
D. Unlimited

Answer: D

NEW QUESTION 34
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 39
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 40
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 45
To improve Splunk performance, parallelIngestionPipelines setting can be adjusted on which of the following components in the Splunk architecture? (Select all that apply.)

A. Indexers
B. Forwarders
C. Search head
D. Cluster master

Answer: AB

NEW QUESTION 47
Which of the following is a best practice to maximize indexing performance?

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

Answer: D

NEW QUESTION 52
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 56
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 61
A Splunk user successfully extracted an ip address into a field called src_ip. Their colleague cannot see that field in their search results with events known to have src_ip. Which of the following may explain the problem? (Select all that apply.)

A. The field was extracted as a private knowledge object.
B. The events are tagged as communicate, but are missing the network tag.
C. The Typing Queue, which does regular expression replacements, is blocked.
D. The colleague did not explicitly use the field in the search and the search was set to Fast Mode.

Answer: D

NEW QUESTION 63
What is the default log size for Splunk internal logs?

A. 10MB
B. 20 MB
C. 25MB
D. 30MB

Answer: C

NEW QUESTION 64
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 67
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 70
.....

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/