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
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 2
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 3
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 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.

Answer: BD

NEW QUESTION 5
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 6
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 7
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 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
To reduce the captain's work load in a search head cluster, what setting will prevent scheduled searches from running on the captain?

A. adhoc_searchhead = true (on all members)
B. adhoc_searchhead = true (on the current captain)
C. captain_is_adhoc_searchhead = true (on all members)
D. captain_is_adhoc_searchhead = true (on the current captain)

Answer: D

NEW QUESTION 10
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 10
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 11
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 12
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 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 16
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 17
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 19
Which command is used for thawing the archive bucket?

A. Splunk collect
B. Splunk convert
C. Splunk rebuild
D. Splunk dbinspect

Answer: C

NEW QUESTION 21
Which of the following is a way to exclude search artifacts when creating a diag?

A. SPLUNK_HOME/bin/splunk diag --exclude
B. SPLUNK_HOME/bin/splunk diag --debug --refresh
C. SPLUNK_HOME/bin/splunk diag --disable=dispatch
D. SPLUNK_HOME/bin/splunk diag --filter-searchstrings

Answer: A

NEW QUESTION 23
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 25
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 28
When adding or decommissioning a member from a Search Head Cluster (SHC), what is the proper order of operations?

A. 1. Delete Splunk Enterprise, if it exists.2. Install and initialize the instance.3. Join the SHC.
B. 1. Install and initialize the instance.2. Delete Splunk Enterprise, if it exists.3. Join the SHC.
C. 1. Initialize cluster rebalance operation.2. Remove master node from cluster.3. Trigger replication.
D. 1. Trigger replication.2. Remove master node from cluster.3. Initialize cluster rebalance operation.

Answer: B

NEW QUESTION 29
Of the following types of files within an index bucket, which file type may consume the most disk?

A. Rawdata
B. Bloom filter
C. Metadata (.data)
D. Inverted index (.tsidx)

Answer: B

NEW QUESTION 33
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

NEW QUESTION 38
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 41
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 43
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 44
When Splunk is installed, where are the internal indexes
stored by default?

A. SPLUNK_HOME/bin
B. SPLUNK_HOME/var/lib
C. SPLUNK_HOME/var/run
D. SPLUNK_HOME/etc/system/default

Answer: B

NEW QUESTION 46
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 49
.....

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/