

Splunk.SPLK-2002.v2023-03-20.q70

Exam Code:	SPLK-2002
Exam Name:	Splunk Enterprise Certified Architect
Certification Provider:	Splunk
Free Question Number:	70
Version:	v2023-03-20
# of views:	837
# of Questions views:	5026
https://www.dumpsfiles.com/files/Splunk/SPLK-2002/Splunk.SPLK-2002.v2023-03-20.q70	

NEW QUESTION: 1

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

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

Answer: C ([LEAVE A REPLY](#))

NEW QUESTION: 2

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

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

Answer: C ([LEAVE A REPLY](#))

NEW QUESTION: 3

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 ([LEAVE A REPLY](#))

Explanation/Reference:

<https://docs.splunk.com/Documentation/Splunk/7.3.2/Admin/Wheretofindtheconfigurationfiles>

NEW QUESTION: 4

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

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

Answer: ([SHOW ANSWER](#))

NEW QUESTION: 5

When troubleshooting monitor inputs, which command checks the status of the tailed files?

- A. splunk cmd btool check inputs layer
- B. curl https://serverhost:8089/services/admin/inputstatus/TailingProcessor:Tailstatus
- C. splunk cmd btool inputs list | tail
- D. curl https://serverhost:8089/services/admin/inputstatus/TailingProcessor:FileStatus

Answer: D ([LEAVE A REPLY](#))

NEW QUESTION: 6

When planning a search head cluster, which of the following is true?

- A. The search head captain must be assigned to the largest search head in the cluster.
- B. All indexers must belong to the underlying indexer cluster (no standalone indexers).
- C. All search heads must be members of the cluster (no standalone search heads).
- D. All search heads must use the same operating system.

Answer: ([SHOW ANSWER](#))

NEW QUESTION: 7

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: A,B,D ([LEAVE A REPLY](#))

Explanation/Reference:

<https://docs.splunk.com/Documentation/Splunk/7.3.2/Indexer/Rebalancethecluster>

NEW QUESTION: 8

Which of the following should be included in a deployment plan?

- A. Business continuity and disaster recovery plans.

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

Answer: D ([LEAVE A REPLY](#))

NEW QUESTION: 9

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: ([SHOW ANSWER](#)**)**

NEW QUESTION: 10

When should multiple search pipelines be enabled?

- A. Only if there are fewer than twelve concurrent users.
- B. Only if disk IOPS is at 800 or better.
- C. Only if CPU and memory resources are significantly under-utilized.
- D. Only if running Splunk Enterprise version 6.6 or later.

Answer: C ([LEAVE A REPLY](#))

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: ([SHOW ANSWER](#)**)**

Explanation/Reference: <https://answers.splunk.com/answers/461939/after-all-clients-are-registered-to-a-deployment-s.html>

NEW QUESTION: 12

The KV store forms its own cluster within a SHC. What is the maximum number of SHC members KV store will

form?

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

Answer: ([SHOW ANSWER](#))

NEW QUESTION: 13

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 ([LEAVE A REPLY](#))

Explanation/Reference:

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

NEW QUESTION: 14

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: ([SHOW ANSWER](#))

Explanation/Reference:

<https://docs.splunk.com/Documentation/Splunk/7.3.2/Indexer/Systemrequirements>

NEW QUESTION: 15

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

Answer: D ([LEAVE A REPLY](#))

NEW QUESTION: 16

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: ([SHOW ANSWER](#))

Explanation/Reference: https://docs.splunk.com/Documentation/Splunk/7.3.2/Capacity/Referencehardware#Reference_host_specification

Valid SPLK-2002 Dumps shared by TrainingDump.com for Helping Passing SPLK-2002 Exam! TrainingDump.com now offer the **newest SPLK-2002 exam dumps**, the TrainingDump.com SPLK-2002 exam **questions have been updated** and **answers have been corrected** get the **newest** TrainingDump.com SPLK-2002 dumps with Test Engine here: <https://www.trainingdump.com/Splunk/SPLK-2002-practice-exam-dumps.html> (207 Q&As Dumps, **40%OFF** Special Discount: **Exam-Tests**)

NEW QUESTION: 17

Which Splunk internal index contains license-related events?

_audit

- A. _license
- B. _internal
- C. _introspection

Answer: ([SHOW ANSWER](#))

Explanation/Reference: <https://answers.splunk.com/answers/579494/how-to-display-license-consumed-by-an-index-over-2.html>

NEW QUESTION: 18

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

Answer: C ([LEAVE A REPLY](#))

NEW QUESTION: 19

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: C ([LEAVE A REPLY](#))

Explanation

<https://docs.splunk.com/Documentation/Splunk/8.1.0/DistSearch/Distsearchsystemrequirements>

NEW QUESTION: 20

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-bundlecommand` from the deployer.
- C. Run the `splunk resync shcluster-replicated-configcommand` on this member.
- D. Run the `clean raftcommand` on all members of the search head cluster.

Answer: B ([LEAVE A REPLY](#))

NEW QUESTION: 21

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 ([LEAVE A REPLY](#))

Explanation/Reference:

<https://docs.splunk.com/Documentation/Splunk/7.3.2/DistSearch/SHCdeploymentoverview>

NEW QUESTION: 22

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

Answer: A ([LEAVE A REPLY](#))

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 ([LEAVE A REPLY](#))

Explanation

NEW QUESTION: 24

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: (SHOW ANSWER)

Explanation/Reference:

<https://docs.splunk.com/Documentation/Splunk/7.3.2/Indexer/Systemrequirements>

NEW QUESTION: 25

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 ([LEAVE A REPLY](#))

NEW QUESTION: 26

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 ([LEAVE A REPLY](#))

Explanation/Reference:

<https://docs.splunk.com/Documentation/Splunk/7.3.2/DistSearch/SHCarchitecture>

NEW QUESTION: 27

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: ([SHOW ANSWER](#))

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

NEW QUESTION: 28

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: ([SHOW ANSWER](#))

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

NEW QUESTION: 29

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 = 3search_factor = 2
- C. replication_factor = 3search_factor = 3
- D. replication_factor = 2search_factor = 3

Answer: B ([LEAVE A REPLY](#))

NEW QUESTION: 30

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

- A. Data source inventory
- B. Deployment schedule
- C. Data policy definition
- D. Topology diagramming

Answer: ([SHOW ANSWER](#))

NEW QUESTION: 31

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: A ([LEAVE A REPLY](#))

Explanation

<https://docs.splunk.com/Documentation/Splunk/7.3.2/DistSearch/SHCarchitecture>

Valid SPLK-2002 Dumps shared by TrainingDump.com for Helping Passing SPLK-2002 Exam! TrainingDump.com now offer the **newest SPLK-2002 exam dumps**, the TrainingDump.com SPLK-2002 exam **questions have been updated** and **answers have been corrected** get the **newest** TrainingDump.com SPLK-2002 dumps with Test Engine here: <https://www.trainingdump.com/Splunk/SPLK-2002-practice-exam-dumps.html> (207 Q&As Dumps, **40%OFF Special Discount: Exam-Tests**)

NEW QUESTION: 32

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: ([SHOW ANSWER](#))

Explanation/Reference: https://docs.splunk.com/Documentation/Splunk/7.3.2/DistSearch/SHCarchitecture#role_of_the_captain

NEW QUESTION: 33

Which of the following are true statements about Splunk indexer clustering?

- A. All peer nodes must run exactly the same Splunk version.
- B. The master node must run the same or a later Splunk version than search heads.
- C. The peer nodes must run the same or a later Splunk version than the master node.
- D. The search head must run the same or a later Splunk version than the peer nodes.

Answer: A ([LEAVE A REPLY](#))

Explanation

<https://docs.splunk.com/Documentation/Splunk/8.1.0/DistSearch/Distsearchsystemrequirements>

NEW QUESTION: 34

Which Splunk Enterprise offering has its own license?

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

Answer: B ([LEAVE A REPLY](#))

NEW QUESTION: 35

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 ([LEAVE A REPLY](#))

Explanation/Reference:

<https://docs.splunk.com/Documentation/Splunk/7.3.2/Indexer/Migratetomultisite>

NEW QUESTION: 36

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: ([SHOW ANSWER](#))

NEW QUESTION: 37

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

Answer: A ([LEAVE A REPLY](#))

NEW QUESTION: 38

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 ([LEAVE A REPLY](#))

Explanation

NEW QUESTION: 39

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 ([LEAVE A REPLY](#))

Explanation/Reference:

<https://docs.splunk.com/Documentation/Splunk/7.3.1/Indexer/Aboutindexesandindexers>

NEW QUESTION: 40

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: (SHOW ANSWER)

Explanation/Reference:

<https://docs.splunk.com/Documentation/Splunk/7.3.2/Indexer/Configuremulti-clustersearch>

NEW QUESTION: 41

What is the algorithm used to determine captancy 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 ([LEAVE A REPLY](#))

Explanation/Reference: <https://answers.splunk.com/answers/664102/need-to-know-about-raft-directory-on-search-head- c.html>

NEW QUESTION: 42

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

Answer: ([SHOW ANSWER](#))

NEW QUESTION: 43

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

replication_factor = 2

A. search_factor = 2

replication_factor = 3

B. search_factor = 2

replication_factor = 2

C. search factor = 3

D. search factor = 3

replication_factor = 3

Answer: **A** ([LEAVE A REPLY](#))

NEW QUESTION: 44

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

A. Decreasing the data model acceleration range.

B. Setting the cluster search factor to N-1.

C. Increasing the number of buckets per index.

D. Setting the cluster replication factor to N-1.

Answer: **D** ([LEAVE A REPLY](#))

NEW QUESTION: 45

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

A. 1. Install and initialize the instance.

2. Delete Splunk Enterprise, if it exists.

3. Join the SHC.

B. 1. Delete Splunk Enterprise, if it exists.

2. Install and initialize the instance.

3. Join the SHC.

C. 1. Trigger replication.

2. Remove master node from cluster.

3. Initialize cluster rebalance operation.

D. 1. Initialize cluster rebalance operation.

2. Remove master node from cluster.

3. Trigger replication.

Answer: ([SHOW ANSWER](#))

NEW QUESTION: 46

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

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

Answer: ([SHOW ANSWER](#))

Valid SPLK-2002 Dumps shared by TrainingDump.com for Helping Passing SPLK-2002 Exam! TrainingDump.com now offer the **newest SPLK-2002 exam dumps**, the TrainingDump.com SPLK-2002 exam **questions have been updated** and **answers have been corrected** get the **newest** TrainingDump.com SPLK-2002 dumps with Test Engine here: <https://www.trainingdump.com/Splunk/SPLK-2002-practice-exam-dumps.html> (207 Q&As Dumps, **40%OFF** Special Discount: **Exam-Tests**)

NEW QUESTION: 47

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 ([LEAVE A REPLY](#))

NEW QUESTION: 48

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. Synchronizes the member list with the KV store primary.
- C. Replicates the SHC's knowledge bundle to the search peers.
- D. Manages alert action suppressions (throttling).

Answer: ([SHOW ANSWER](#))

NEW QUESTION: 49

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 ([LEAVE A REPLY](#))

Explanation/Reference: <https://answers.splunk.com/answers/147951/what-is-the-compression-ratio-of-raw-data-in-splunk.html>

NEW QUESTION: 50

Which of the following is an indexer clustering requirement?

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

Answer: ([SHOW ANSWER](#))

NEW QUESTION: 51

Configurations from the deployer are merged into which location on the search head cluster member?

- A. SPLUNK_HOME/etc/apps/APP_HOME/default
- B. SPLUNK_HOME/etc/apps/search/default
- C. SPLUNK_HOME/etc/apps/APP_HOME/local
- D. SPLUNK_HOME/etc/system/local

Answer: D ([LEAVE A REPLY](#))

NEW QUESTION: 52

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 ([LEAVE A REPLY](#))

Explanation/Reference:

NEW QUESTION: 53

In which phase of the Splunk Enterprise data pipeline are indexed extraction configurations processed?

- A. Indexing
- B. Parsing
- C. Search
- D. Input

Answer: ([SHOW ANSWER](#))

NEW QUESTION: 54

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 ([LEAVE A REPLY](#))

Explanation/Reference:

<https://docs.splunk.com/Documentation/Splunk/7.3.2/DistSearch/SHCarchitecture>

NEW QUESTION: 55

Which of the following commands is used to clear the KV store?

- A. splunk clean kvstore
- B. splunk clear kvstore
- C. splunk delete kvstore
- D. splunk reinitialize kvstore

Answer: ([SHOW ANSWER](#))

NEW QUESTION: 56

Which of the following should be done when installing Enterprise Security on a Search Head Cluster? (Select all that apply.)

- A. Install Enterprise Security on the deployer.
- B. Install Enterprise Security on a staging instance.
- C. Copy the Enterprise Security configurations to the deployer.
- D. Use the deployer to deploy Enterprise Security to the cluster members.

Answer: ([SHOW ANSWER](#))

Explanation/Reference:

<https://docs.splunk.com/Documentation/ES/5.3.1/Install/InstallEnterpriseSecuritySHC>

NEW QUESTION: 57

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 ([LEAVE A REPLY](#))

Explanation/Reference: <https://docs.splunk.com/Documentation/Splunk/7.3.2/Capacity/Accommodatemany simultaneous searches>

NEW QUESTION: 58

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

Answer: A ([LEAVE A REPLY](#))

NEW QUESTION: 59

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: A,B ([LEAVE A REPLY](#))

Explanation/Reference:

<https://docs.splunk.com/Documentation/Splunk/7.3.2/Indexer/Enableclustersindetail>

NEW QUESTION: 60

What is the default log size for Splunk internal logs?

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

Answer: ([SHOW ANSWER](#))

Explanation/Reference: <https://answers.splunk.com/answers/959/how-can-i-control-the-size-and-number-of-splunks-internal-logs.html>

NEW QUESTION: 61

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

- A. polling_interval attribute in deploymentclient.conf
- B. phoneHomeIntervalInSecs attribute in outputs.conf
- C. phoneHomeIntervalInSecs attribute in deploymentclient.conf

D. polling_interval attribute in outputs.conf

Answer: ([SHOW ANSWER](#))

Valid SPLK-2002 Dumps shared by TrainingDump.com for Helping Passing SPLK-2002 Exam! TrainingDump.com now offer the **newest SPLK-2002 exam dumps**, the TrainingDump.com SPLK-2002 exam **questions have been updated** and **answers have been corrected** get the **newest** TrainingDump.com SPLK-2002 dumps with Test Engine here: <https://www.trainingdump.com/Splunk/SPLK-2002-practice-exam-dumps.html> (207 Q&As Dumps, **40%OFF** Special Discount: **Exam-Tests**)

NEW QUESTION: 62

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: ([SHOW ANSWER](#))

NEW QUESTION: 63

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 ([LEAVE A REPLY](#))

Explanation/Reference:

<https://docs.splunk.com/Documentation/Splunk/7.3.2/Admin/Distdeploylicenses>

NEW QUESTION: 64

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 ([LEAVE A REPLY](#))

Explanation/Reference: <https://docs.splunk.com/Documentation/ITSI/4.3.1/Install/Plan>

NEW QUESTION: 65

Which command is used for thawing the archive bucket?

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

Answer: D ([LEAVE A REPLY](#))

NEW QUESTION: 66

Which of the following should be done when installing Enterprise Security on a Search Head Cluster? (Select all that apply.)

- A. Install Enterprise Security on the deployer.
- B. Install Enterprise Security on a staging instance.
- C. Copy the Enterprise Security configurations to the deployer.
- D. Use the deployer to deploy Enterprise Security to the cluster members.

Answer: (SHOW ANSWER)

Explanation/Reference:

<https://docs.splunk.com/Documentation/ES/5.3.1/Install/InstallEnterpriseSecuritySHC>

NEW QUESTION: 67

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: (SHOW ANSWER)

Explanation/Reference: <https://answers.splunk.com/answers/479312/how-to-edit-inputsconf-to-monitor-multiple-files-w-1.html>

NEW QUESTION: 68

Which of the following can a Splunk diag contain?

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

Answer: D ([LEAVE A REPLY](#))

NEW QUESTION: 69

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 ([LEAVE A REPLY](#))

Explanation/Reference:

<https://docs.splunk.com/Documentation/Splunk/7.3.2/Indexer/Decommissionasite>

NEW QUESTION: 70

Which of the following options can improve reliability of syslog delivery to Splunk? (Select all that apply.)

- A. Use a network load balancer to direct syslog traffic to active backend syslog listeners.
- B. Use one or more syslog servers to persist data with a Universal Forwarder to send the data to Splunk indexers.
- C. Configure UDP inputs on each Splunk indexer to receive data directly.
- D. Use TCP syslog.

Answer: ([SHOW ANSWER](#))

Valid SPLK-2002 Dumps shared by TrainingDump.com for Helping Passing SPLK-2002 Exam! TrainingDump.com now offer the **newest SPLK-2002 exam dumps**, the TrainingDump.com SPLK-2002 exam **questions have been updated** and **answers have been corrected** get the **newest** TrainingDump.com SPLK-2002 dumps with Test Engine here: <https://www.trainingdump.com/Splunk/SPLK-2002-practice-exam-dumps.html> (207 Q&As Dumps, **40%OFF** Special Discount: **Exam-Tests**)