



# Splunk

## Exam Questions SPLK-2002

Splunk Enterprise Certified Architect

#### 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

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 4

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 5

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 6

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 7

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 8

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 9

Which Splunk server role regulates the functioning of indexer cluster?

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

**Answer:** C

#### NEW QUESTION 10

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 10

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 14

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

- A. polling\_interval attribute in outputs.conf
- B. phoneHomeIntervalInSecs attribute in outputs.conf
- C. polling\_interval attribute in deploymentclient.conf
- D. phoneHomeIntervalInSecs attribute in deploymentclient.conf

**Answer:** D

#### NEW QUESTION 18

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 19

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 23

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 28

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 29

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 31

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 36

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 40

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 45

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 48

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 52

Which of the following statements describe licensing in a clustered Splunk deployment? (Select all that apply.)

- A. Free licenses do not support clustering.
- B. Replicated data does not count against licensing.
- C. Each cluster member requires its own clustering license.
- D. Cluster members must share the same license pool and license master.

**Answer:** BD

#### NEW QUESTION 55

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 58

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 60

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 65

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 68

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 69

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 71

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 74

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 76

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 78

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 82

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 86

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 87

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 91

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 96

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 98

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 100

.....

## 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

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

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 4

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 5

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 6

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 7

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 8

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 9

Which Splunk server role regulates the functioning of indexer cluster?

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

**Answer:** C

#### NEW QUESTION 10

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 10

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 14

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

- A. polling\_interval attribute in outputs.conf
- B. phoneHomeIntervalInSecs attribute in outputs.conf
- C. polling\_interval attribute in deploymentclient.conf
- D. phoneHomeIntervalInSecs attribute in deploymentclient.conf

**Answer:** D

#### NEW QUESTION 18

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 19

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 23

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 28

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 29

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 31

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 36

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 40

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 45

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 48

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 52

Which of the following statements describe licensing in a clustered Splunk deployment? (Select all that apply.)

- A. Free licenses do not support clustering.
- B. Replicated data does not count against licensing.
- C. Each cluster member requires its own clustering license.
- D. Cluster members must share the same license pool and license master.

**Answer:** BD

#### NEW QUESTION 55

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 58

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 60

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 65

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 68

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 69

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 71

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 74

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 76

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 78

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 82

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 86

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 87

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 91

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 96

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 98

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 100

.....

## 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/>