CertsCare

Free Questions for SPLK-2002 by certscare

Shared by Banks on 12-12-2023

For More Free Questions and Preparation Resources

Check the Links on Last Page

Question 1

Question Type: MultipleChoice

What is the logical first step when starting a deployment plan?

Options:

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

Question 2

Question Type: MultipleChoice

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

Options:

A- Use TCP syslog.

B- Configure UDP inputs on each Splunk indexer to receive data directly.

C- Use a network load balancer to direct syslog traffic to active backend syslog listeners.

D- Use one or more syslog servers to persist data with a Universal Forwarder to send the data to Splunk indexers.

Answer:

C, D

Question 3

Question Type: **MultipleChoice**

When Splunk is installed. where are the internal indexes stored by default?

Options:

A- SPLUNK_HOME/bin

B- SPLUNK_HOME/var/lib

C- SPLUNK_HOME/var/run

D- SPLUNK_HOME/etc/system/default

Answer:

B

Question 4

Question Type: **MultipleChoice**

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

Options:

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

Question 5

Question Type: MultipleChoice

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

Options:

A- replication_factor = 2search_factor = 2

B- replication_factor = 2search factor = 3

C- replication_factor = 3search_factor = 2

D- replication_factor = 3search factor = 3

Answer:

A

Question 6

Question Type: MultipleChoice

Consider a use case involving firewall dat

a. There is no Splunk-supported Technical Add-On, but the vendor has built one. What are the items that must be evaluated before installing the add-on? (Select all that apply.)

Options:

A- Identify number of scheduled or real-time searches.

B- Validate if this Technical Add-On enables event data for a data model.

C- Identify the maximum number of forwarders Technical Add-On can support.

D- Verify if Technical Add-On needs to be installed onto both a search head or indexer.

Answer:

A, C

Question 7

Question Type: **MultipleChoice**

In a distributed environment, knowledge object bundles are replicated from the search head to which location on the search peer(s)?

Options:

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

Question 8

Question Type: MultipleChoice

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

Options:

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

Question 9

Question Type: MultipleChoice

As a best practice, where should the internal licensing logs be stored?

Options:

A- Indexing layer.

B- License server.

C- Deployment layer.

D- Search head layer.

Answer:

D

Question 10

Question Type: **MultipleChoice**

Which of the following statements about integrating with third-party systems is true? (Select all that apply.)

Options:

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:

C, D

Question 11

Question Type: **MultipleChoice**

What is the algorithm used to determine captaincy in a Splunk search head cluster?

Options:

A- Raft distributed consensus.

B- Rapt distributed consensus.

C- Rift distributed consensus.

D- Round-robin distribution consensus.

Answer:

A

Question 12

Question Type: MultipleChoice

Which of the following is an indexer clustering requirement?

Options:

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

20%
DISCOUNT