Free Questions for SPLK-2002 by go4braindumps

Shared by Norton on 06-06-2022

For More Free Questions and Preparation Resources

Check the Links on Last Page

Question 1

Question Type: **MultipleChoice**

Because Splunk indexing is read/write intensive, it is important to select the appropriate disk storage solution for each deployment. Which of the following statements is accurate about disk storage?

Options:

A- High performance SAN should never be used.

B- Enable NFS for storing hot and warm buckets.

C- The recommended RAID setup is RAID 10 (1 + 0).

D- Virtualized environments are usually preferred over bare metal for Splunk indexers.

Answer:

C

Question 2

Question Type: **MultipleChoice**

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

Options:

A- Use case checklist.

B- Install Splunk apps.

C- Inventory data sources.

D- Review network topology.

Answer:

D

Question 3

Question Type: MultipleChoice

Which of the following statements describe search head clustering? (Select all that apply.)

Options:

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:

A, C

Question 4

Question Type: **MultipleChoice**

What is the default log size for Splunk internal logs?

Options:

A- 10MB

B- 20 MB

C- 25MB

D- 30MB

Answer:

C

Question 5

Question Type: **MultipleChoice**

Which two sections can be expanded using the Search Job Inspector?

Options:

A- Execution costs.

B- Saved search history.

C- Search job properties.

D- Optimization suggestions.

Answer:

B, C

Question 6

Question Type: **MultipleChoice**

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.)

Options:

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