Up-to-date Questions and Answers from authentic resources to improve knowledge and pass the exam at very first attempt. ----- Guaranteed.

Splunk

SPLK-3003

Splunk Core Certified Consultant

https://killexams.com/pass4sure/exam-detail/SPLK-3003

Question #76

A customer would like to remove the output_file capability from users with the default user role to stop them from filling up the disk on the search head with lookup files. What is the best way to remove this capability from users?

- A. Create a new role without the output_file capability that inherits the default user role and assign it to the users.
- B. Create a new role with the output_file capability that inherits the default user role and assign it to the users.
- C. Edit the default user role and remove the output_file capability.
- D. Clone the default user role, remove the output_file capability, and assign it to the users.

Answer: C

Question #77

A working search head cluster has been set up and used for 6 months with just the native/local Splunk user authentication method. In order to integrate the search heads with an external Active Directory server using LDAP, which of the following statements represents the most appropriate method to deploy the configuration to the servers?

- A. Configure the integration in a base configuration app located in shcluster-apps directory on the search head deployer, then deploy the configuration to the search heads using the splunk apply shcluster-bundle command.
- B. Log onto each search using a command line utility. Modify the authentication.conf and authorize.conf files in a base configuration app to configure the integration.
- C. Configure the LDAP integration on one Search Head using the Settings > Access Controls > Authentication Method and Settings > Access Controls > Roles Splunk UI menus. The configuration setting will replicate to the other nodes in the search head cluster eliminating the need to do this on the other search heads.
- D. On each search head, login and configure the LDAP integration using the Settings > Access Controls > Authentication Method and Settings > Access Controls > Roles Splunk UI menus.

Answer: C
Reference:
https://docs.splunk.com/Documentation/Splunk/8.1.0/Security/ConfigureLDAPwithSplunkWeb

Question #78

In an environment that has Indexer Clustering, the Monitoring Console (MC) provides dashboards to monitor environment health. As the environment grows over time and new indexers are added, which steps would ensure the MC is aware of the additional indexers?

- A. No changes are necessary, the Monitoring Console has self-configuration capabilities.
- B. Using the MC setup UI, review and apply the changes.
- C. Remove and re-add the cluster master from the indexer clustering UI page to add new peers, then apply the changes under the MC setup UI.
- D. Each new indexer needs to be added using the distributed search UI, then settings must be saved under the MC setup UI.

Answer: B

Question #79

In addition to the normal responsibilities of a search head cluster captain, which of the following is a default behavior?

- A. The captain is not a cluster member and does not perform normal search activities.
- B. The captain is a cluster member who performs normal search activities.
- C. The captain is not a cluster member but does perform normal search activities.
- D. The captain is a cluster member but does not perform normal search activities.

Answer: B
Reference:
https://docs.splunk.com/Documentation/Splunk/8.1.0/DistSearch/SHCarchitecture#Search_head_cluster_captain

Question #80

What happens to the indexer cluster when the indexer Cluster Master (CM) runs out of disk space?

- A. A warm standby CM needs to be brought online as soon as possible before an indexer has an outage.
- B. The indexer cluster will continue to operate as long as no indexers fail.
- C. If the indexer cluster has site failover configured in the CM, the second cluster master will take over.
- D. The indexer cluster will continue to operate as long as a replacement CM is deployed within 24 hours.

Answer: C

Question #81

Which event processing pipeline contains the regex replacement processor that would be called upon to run event masking routines on events as they are ingested?

- A. Merging pipeline
- B. Indexing pipeline
- C. Typing pipeline
- D. Parsing pipeline

Answer: A

Question #82

Which statement is correct?

- A. In general, search commands that can be distributed to the search peers should occur as early as possible in a well-tuned search.
- B. As a streaming command, streamstats performs better than stats since stats is just a reporting command.
- C. When trying to reduce a search result to unique elements, the dedup command is the only way to achieve this.
- D. Formatting commands such as fieldformat should occur as early as possible in the search to take full advantage of the often larger number of search peers.

Answer: D

Question #83

A non-ES customer has a concern about data availability during a disaster recovery event. Which of the following Splunk Validated Architectures (SVAs) would be recommended for that use case?

- A. Topology Category Code: M4
- B. Topology Category Code: M14
- C. Topology Category Code: C13
- D. Topology Category Code: C3

Answer: B
Reference:
https://www.splunk.com/pdfs/technical-briefs/splunk-validated-architectures.pdf
(21)

Question #84

The universal forwarder (UF) should be used whenever possible, as it is smaller and more efficient. In which of the following scenarios would a heavy forwarder
(HF) be a more appropriate choice?

- A. When a predictable version of Python is required.
- B. When filtering 10%""15% of incoming events.
- C. When monitoring a log file.

D. When running a script.

Answer: B
Reference:
https://www.splunk.com/en_us/blog/tips-and-tricks/universal-or-heavy-that-is-the-question.html

Question #85

When monitoring and forwarding events collected from a file containing unstructured textual events, what is the difference in the Splunk2Splunk payload traffic sent between a universal forwarder (UF) and indexer compared to the Splunk2Splunk payload sent between a heavy forwarder (HF) and the indexer layer?
(Assume that the file is being monitored locally on the forwarder.)

- A. The payload format sent from the UF versus the HF is exactly the same. The payload size is identical because they're both sending 64K chunks.
- B. The UF sends a stream of data containing one set of medata fields to represent the entire stream, whereas the HF sends individual events, each with their own metadata fields attached, resulting in a lager payload.
- C. The UF will generally send the payload in the same format, but only when the sourcetype is specified in the inputs.conf and EVENT_BREAKER_ENABLE is set to true.
- D. The HF sends a stream of 64K TCP chunks with one set of metadata fields attached to represent the entire stream, whereas the UF sends individual events, each with their own metadata fields attached.

Answer: B