Free Questions for SPLK-3003 by certsdeals

Shared by Burgess on 12-12-2023

For More Free Questions and Preparation Resources

Check the Links on Last Page

Question 1

Question Type: MultipleChoice

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?

Options:

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

Question 2

Question Type: MultipleChoice

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?

Options:

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 3

Question Type: MultipleChoice

A customer has 30 indexers in an indexer cluster configuration and two search heads. They are working on writing SPL search for a particular use-case, but are concerned that it takes too long to run for short time durations.

How can the Search Job Inspector capabilities be used to help validate and understand the customer concerns?

Options:

A- Search Job Inspector provides statistics to show how much time and the number of events each indexer has processed.

B- Search Job Inspector provides a Search Health Check capability that provides an optimized SPL query the customer should try instead.

C- Search Job Inspector cannot be used to help troubleshoot the slow performing search; customer should review index=_introspection instead.

D- The customer is using the transaction SPL search command, which is known to be slow.

Answer:

A

Question 4

Question Type: MultipleChoice

Which of the following is the most efficient search?

A.
```
index=foo sourcetype=bar | lookup local=t mylookup host OUTPUT
host_flag | where host_flag= "true" | stats count by host
```

B.
```
index=foo sourcetype=* | lookup mylookup host OUTPUT
host_flag | where host_flag= "true" | stats count by host
```

C.
```
index=foo sourcetype=bar | fields host | lookup mylookup host OUTPUT
host_flag | where host_flag= "true" | stats count by host
```

D.
```
index=foo sourcetype=bar | table host | lookup local=t mylookup host OUTPUT
host_flag | where host_flag= "true" | stats count by host
```

Options:

A- Option A

B- Option B

C- Option C

D- Option D

Answer:

C

Question 5

Question Type: MultipleChoice

In a large cloud customer environment with many (>100) dynamically created endpoint systems, each with a UF already deployed, what is the best approach for associating these systems with an appropriate serverclass on the deployment server?

Options:

A- Work with the cloud orchestration team to create a common host-naming convention for these systems so a simple pattern can be used in the serverclass.conf whitelist attribute.

B- Create a CSV lookup file for each severclass, manually keep track of the endpoints within this CSV file, and leverage the whitelist.from_pathname attribute in serverclass.conf.

C- Work with the cloud orchestration team to dynamically insert an appropriate clientName setting into each endpoint's local/deploymentclient.conf which can be matched by whitelist in serverclass.conf.

D- Using an installation bootstrap script run a CLI command to assign a clientName setting and permit serverclass.conf whitelist simplification.

Answer:

C

Question 6

Question Type: MultipleChoice

The Splunk Validated Architectures (SVAs) document provides a series of approved Splunk topologies. Which statement accurately describes how it should be used by a customer?

Options:

A- Customer should look at the category tables, pick the highest number that their budget permits, then select this design topology as the chosen design.

B- Customers should identify their requirements, provisionally choose an approved design that meets them, then consider design principles and best practices to come to an informed design decision.

C- Using the guided requirements gathering in the SVAs document, choose a topology that suits requirements, and be sure not to deviate from the specified design.

D- Choose an SVA topology code that includes Search Head and Indexer Clustering because it offers the highest level of resilience.

Answer:

B

Question 7

Question Type: MultipleChoice

Which of the following server roles should be configured for a host which indexes its internal logs locally?

Options:

A- Cluster master

B- Indexer

C- Monitoring Console (MC)

D- Search head

Answer:

B

Question 8

Question Type: MultipleChoice

When using SAML, where does user authentication occur?

Options:

A- Splunk generates a SAML assertion that authenticates the user.

B- The Service Provider (SP) decodes the SAML request and authenticates the user.

C- The Identity Provider (IDP) decodes the SAML request and authenticates the user.

D- The Service Provider (SP) generates a SAML assertion that authenticates the user.

Answer:

A

Question 9

Question Type: MultipleChoice

A customer is migrating their existing Splunk Indexer from an old set of hardware to a new set of indexers. What is the earliest method to migrate the system?

Options:

A- 1. Add new indexers to the cluster as peers, in the same site (if needed).
2. Ensure new indexers receive common configuration.
3. Decommission old indexers (one at a time) to allow time for CM to fix/migrate buckets to new hardware.
4. Remove all the old indexers from the CM's list.

B- 1. Add new indexers to the cluster as peers, to a new site.
2. Ensure new indexers receive common configuration from the CM.
3. Decommission old indexers (one at a time) to allow time for CM to fix/migrate buckets to new hardware.
4. Remove all the old indexers from the CM's list.

C- 1. Add new indexers to the cluster as peers, in the same site.
2. Update the replication factor by +1 to Instruct the cluster to start replicating to new peers.
3. Allow time for CM to fix/migrate buckets to new hardware.
4. Remove all the old indexers from the CM's list.

D- 1. Add new indexers to the cluster as new site.
2. Update cluster master (CM) server.conf to include the new available site.
3. Allow time for CM to fix/migrate buckets to new hardware.
4. Remove the old indexers from the CM's list.

Answer:

B

Question 10

Question Type: MultipleChoice

When utilizing a subsearch within a Splunk SPL search query, which of the following statements is accurate?

Options:

A- Subsearches have to be initiated with the | subsearch command.

B- Subsearches can only be utilized with | inputlookup command.

C- Subsearches have a default result output limit of 10000.

D- There are no specific limitations when using subsearches.

Answer:

C

Question 11

Question Type: MultipleChoice

A customer is using both internal Splunk authentication and LDAP for user management.

If a username exists in both $SPLUNK_HOME/etc/passwd and LDAP, which of the following statements is accurate?

Options:

A- The internal Splunk authentication will take precedence.

B- Authentication will only succeed if the password is the same in both systems.

C- The LDAP user account will take precedence.

D- Splunk will error as it does not support overlapping usernames

Answer:

A

Question 12

Question Type: **MultipleChoice**

When setting up a multisite search head and indexer cluster, which nodes are required to declare site membership?

Options:

A- Search head cluster members, deployer, indexers, cluster master

B- Search head cluster members, deployment server, deployer, indexers, cluster master

C- All splunk nodes, including forwarders, must declare site membership

D- Search head cluster members, indexers, cluster master

Answer:

D