Free Questions for SPLK-3003 by braindumpscollection

Shared by Rhodes on 15-04-2024

For More Free Questions and Preparation Resources

Check the Links on Last Page

Question 1

Question Type: MultipleChoice

What is required to setup the HTTP Event Collector (HEC)?

Options:

A- Each HEC input requires a unique name but token values can be shared.

B- Each HEC input requires an existing forwarder output group.

C- Each HEC input entry must contain a valid token.

D- Each HEC input requires a Source name field.

Answer:

C

Question 2

Question Type: MultipleChoice

A new search head cluster is being implemented. Which is the correct command to initialize the deployer node without restarting the search head cluster peers?

Options:

A- $SPLUNK_HOME/bin/splunk apply shcluster-bundle

B- $SPLUNK_HOME/bin/splunk apply cluster-bundle

C- $SPLUNK_HOME/bin/splunk apply shcluster-bundle --action stage

D- $SPLUNK_HOME/bin/splunk apply cluster-bundle --action stage

Answer:

A

Question 3

Question Type: **MultipleChoice**

A new single-site three indexer cluster is being stood up with replication_factor:2, search_factor:2. At which step would the Indexer Cluster be classed as 'Indexing Ready' and be able to ingest new data?

Step 1: Install and configure Cluster Master (CM)/Master Node with base clustering stanza settings, restarting CM.

Step 2: Configure a base app in etc/master-apps on the CM to enable a splunktcp input on port 9997 and deploy index creation configurations.

Step 3: Install and configure Indexer 1 so that once restarted, it contacts the CM, download the latest config bundle.

Step 4: Indexer 1 restarts and has successfully joined the cluster.

Step 5: Install and configure Indexer 2 so that once restarted, it contacts the CM, downloads the latest config bundle

Step 6: Indexer 2 restarts and has successfully joined the cluster.

Step 7: Install and configure Indexer 3 so that once restarted, it contacts the CM, downloads the latest config bundle.

Step 8: Indexer 3 restarts and has successfully joined the cluster.

Options:

A- Step 2

B- Step 4

C- Step 6

D- Step 8

Answer:

A

Question 4

Question Type: MultipleChoice

A customer has a number of inefficient regex replacement transforms being applied. When under heavy load the indexers are struggling to maintain the expected indexing rate. In a worst case scenario, which queue(s) would be expected to fill up?

Options:

A- Typing, merging, parsing, input

B- Parsing

C- Typing

D- Indexing, typing, merging, parsing, input

Answer:

B

Question 5

Question Type: MultipleChoice

A customer wants to migrate from using Splunk local accounts to use Active Directory with LDAP for their Splunk user accounts instead. Which configuration files must be modified to connect to an Active Directory LDAP provider?

Options:

A- authentication.conf, authorize.conf, ldap.conf

B- authentication.conf, ldap.conf

C- authentication.conf

D- authorize.conf, authentication.conf

Answer:

C

Question 6

Question Type: MultipleChoice

When adding a new search head to a search head cluster (SHC), which of the following scenarios occurs?

Options:

A- The new search head connects to the captain and replays any recent configuration changes to bring it up to date.

B- The new search head connects to the deployer and replays any recent configuration changes to bring it up to date.

C- The new search head connects to the captain and pulls the most recently deployed bundle. It then connects to the deployer and replays any recent configuration changes to bring it up to date.

D- The new search head connects to the deployer and pulls the most recently deployed bundle. It then connects to the captain and replays any recent configuration changes to bring it up to date.

Answer:

C

Question 7

Question Type: MultipleChoice

As a best practice which of the following should be used to ingest data on clustered indexers?

Options:

A- Monitoring (via a process), collecting data (modular inputs) from remote systems/applications

B- Modular inputs, HTTP Event Collector (HEC), inputs.conf monitor stanza

C- Actively listening on ports, monitoring (via a process), collecting data from remote systems/applications

D- splunktcp, splunktcp-ssl, HTTP Event Collector (HEC)

Answer:

B

Question 8

Question Type: **MultipleChoice**

In which directory should base config app(s) be placed to initialize an indexer?

Options:

A- $SPLUNK_HOME/etc/

B- $SPLUNK_HOME/etc/apps

C- $SPLUNK_HOME/etc/system/local

D- $SPLUNK_HOME/etc/slave-apps

Answer:

B

Question 9

Question Type: MultipleChoice

A customer would like Splunk to delete files after they've been ingested. The Universal Forwarder has read/ write access to the directory structure. Which input type would be most appropriate to use in order to ensure files are ingested and then deleted afterwards?

Options:

A- Script

B- Batch

C- Monitor

D- Fschange

Answer:

B

Question 10

Question Type: MultipleChoice

A customer has implemented their own Role Based Access Control (RBAC) model to attempt to give the Security team different data access than the Operations team by creating two new Splunk roles -- security and operations. In the srchIndexesAllowed setting of authorize.conf, they specified the network index

under the security role and the operations index under the operations role. The new roles are set up to inherit the default user role.

If a new user is created and assigned to the operations role only, which indexes will the user have access to search?

Options:

A- operations, network, _internal, _audit

B- operations

C- No Indexes

D- operations, network

Answer:

A

Question 11

Question Type: MultipleChoice

In which of the following scenarios is a subsearch the most appropriate?

Options:

A- When joining results from multiple indexes.

B- When dynamically filtering hosts.

C- When filtering indexed fields.

D- When joining multiple large datasets.

Answer:

A