Free Questions for SPLK-1003 by braindumpscollection

Shared by Sloan on 20-10-2022

For More Free Questions and Preparation Resources

Check the Links on Last Page

Question 1

Question Type: MultipleChoice

Which setting allows the configuration of Splunk to allow events to span over more than one line?

Options:

A- SHOULD_LINEMERGE = true

B- BREAK_ONLY_BEFORE_DATE = true

C- BREAK_ONLY_BEFORE = <REGEX pattern>

D- SHOULD_LINEMERGE = false

Answer:

C

Question 2

Question Type: MultipleChoice

What is the command to reset the fishbucket for one source?

Options:

A- rm -r ~/splunkforwarder/var/lib/splunk/fishbucket

B- splunk clean eventdata -index _thefishbucket

C- splunk cmd btprobe -d SPLUNK_HOME/var/lib/splunk/fishbucket/splunk_private_db --file <source> --reset

D- splunk btool fishbucket reset <source>

Answer:

C

Question 3

Question Type: MultipleChoice

In addition to single, non-clustered Splunk instances, what else can the deployment server push apps to?

Options:

A- Universal forwarders

B- Splunk Cloud

C- Linux package managers

D- Windows using WMI

Answer:

A

Question 4

Question Type: MultipleChoice

All search-time field extractions should be specified on which Splunk component?

Options:

A- Deployment server

B- Universal forwarder

C- Indexer

D- Search head

Answer:

C

Question 5

Question Type: MultipleChoice

Which artifact is required in the request header when creating an HTTP event?

Options:

A- ackID

B- Token

C- Manifest

D- Host name

Answer:

B

Question 6

Question Type: **MultipleChoice**

Using the CLI on the forwarder, how could the current forwarder to indexer configuration be viewed?

Options:

A- splunk btool server list --debug

B- splunk list forward-indexer

C- splunk list forward-server

D- splunk btool indexes list --debug

Answer:

C

Question 7

Question Type: MultipleChoice

When Splunk is integrated with LDAP, which attribute can be changed in the Splunk UI for an LDAP user?

Options:

A- Default app

B- LDAP group

C- Password

D- Username

Answer:

B

Question 8

Question Type: MultipleChoice

Which default Splunk role could be assigned to provide users with the following capabilities?

Create saved searches

Edit shared objects and alerts

Not allowed to create custom roles

Options:

A- admin

B- power

C- user

D- splunk-system-role

Answer:

B

Question 9

Question Type: **MultipleChoice**

Which of the following is a valid distributed search group?

Options:

A- [distributedSearch:Paris] default = false servers = server1, server2

B- [searchGroup:Paris] default = false servers = server1:8089, server2:8089

C- [searchGroup:Paris] default = false servers = server1:9997, server2:9997

D- [distributedSearch:Paris] default = false servers = server1:8089; server2:8089

Answer:

D