SPLK-1003 Q&As

Splunk Enterprise Certified Admin

Pass Splunk SPLK-1003 Exam with 100% Guarantee

Free Download Real Questions & Answers **PDF** and **VCE** file from:

https://www.passapply.com/splk-1003.html

100% Passing Guarantee
100% Money Back Assurance

Following Questions and Answers are all new published by Splunk Official Exam Center

- **Instant Download** After Purchase
- **100% Money Back** Guarantee
- **365 Days** Free Update
- **800,000+** Satisfied Customers

QUESTION 1

UsingSEDCMDinprops.confallows raw data to be modified. With the given event below, which option will mask the first three digits of theAcctIDfield resulting output:[22/Oct/2018:15:50:21] VendorID=1234 Code=B AcctID=xxx5309 Event: [22/Oct/2018:15:50:21] VendorID=1234 Code=B AcctID=xxx5309

A. SEDCMD-1acct = s/VendorID=\d{3}(\d{4})/VendorID=xxx/g

B. SEDCMD-xxxAcct = s/AcctID=\d{3}(\d{4})/AcctID=xxx/g

C. SEDCMD-1acct = s/AcctID=\d{3}(\d{4})/AcctID=\1xxx/g

D. SEDCMD-1acct = s/AcctID=\d{3}(\d{4})/AcctID=xxx\1/g

Correct Answer: D

https://docs.splunk.com/Documentation/Splunk/8.2.2/Data/Anonymizedata Scrolling down to the section titled "Define the sed script in props.conf shows the correct syntax of an example which validates that the number/character /1 immediately preceded the /g

QUESTION 2

When configuring HTTP Event Collector (HEC) input, how would one ensure the events have been indexed?

A. Enable indexer acknowledgment.

B. Enable forwarder acknowledgment.

C. splunk check-integrity -index

D. index=_internal component=ACK | stats count by host

Correct Answer: A

Per the provided Splunk reference URL https://docs.splunk.com/Documentation/Splunk/8.0.5/Data/AboutHECIDXAck

"While HEC has precautions in place to prevent data loss, it\\'s impossible to completely prevent such an occurrence, especially in the event of a network failure or hardware crash. This is where indexer acknolwedgment comes in."

Reference https://docs.splunk.com/Documentation/Splunk/8.0.5/Data/AboutHECIDXAck

QUESTION 3

How do you remove missing forwarders from the Monitoring Console?

A. By restarting Splunk.

B. By rescanning active forwarders.

C. By reloading the deployment server.

D. By rebuilding the forwarder asset table.

Correct Answer: D

QUESTION 4

Which of the following are required when defining an index in indexes. conf? (select all that apply)

A. coldPath

B. homePath

C. frozenPath

D. thawedPath

Correct Answer: ABD

homePath = $SPLUNK_DB/hatchdb/db coldPath = $SPLUNK_DB/hatchdb/colddb thawedPath = $SPLUNK_DB/hatchdb/thaweddb

QUESTION 5

Which of the following methods will connect a deployment client to a deployment server? (select all that apply)

A. Run $SPLUNK_ROME/bin/ splunk set deploy-poll : from the command line of the deployment client.

B. Create and edit a deploymentserver . conf file in SSPLVNE{ on the deployment server.

C. Create and edit a deploymentclient . conf file in SSPLTJNE(EOME/etc/ system/local on the deployment client.

D. Run $SPLUNK ROME/bin/spiunk set deploy-poi i : from the command line of the deployment server.

Correct Answer: AC

The correct methods to connect a deployment client to a deployment server are A and C. You can either run the command splunk set deploy-poll : from the command line of the deployment client1 or create and edit a deploymentclient.conf file in $SPLUNK_HOME/etc/system/local on the deployment client2. Both methods require you to specify the IP address, hostname, and management port of the deployment server that you want the client to connect to.