SPLK-3003$^{\text{Q\&As}}$

Splunk Core Certified Consultant

Pass Splunk SPLK-3003 Exam with 100% Guarantee

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

https://www.geekcert.com/splk-3003.html

100% Passing Guarantee
100% Money Back Assurance

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

QUESTION 1

A customer has been using Splunk for one year, utilizing a single/all-in-one instance. This single Splunk server is now struggling to cope with the daily ingest rate. Also, Splunk has become a vital system in dayto-day operations making high availability a consideration for the Splunk service. The customer is unsure how to design the new environment topology in order to provide this.

Which resource would help the customer gather the requirements for their new architecture?

A. Direct the customer to the docs.splunk.com and tell them that all the information to help them select the right design is documented there.

B. Ask the customer to engage with the sales team immediately as they probably need a larger license.

C. Refer the customer to answers.splunk.com as someone else has probably already designed a system that meets their requirements.

D. Refer the customer to the Splunk Validated Architectures document in order to guide them through which approved architectures could meet their requirements.

Correct Answer: D

Reference: https://www.splunk.com/pdfs/technical-briefs/splunk-validated-architectures.pdf

QUESTION 2

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?

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.

Correct Answer: C

QUESTION 3

A customer is using regex to whitelist access logs and secure logs from a web server, but only the access logs are being ingested. Which troubleshooting resource would provide insight into why the secure logs are not being ingested?

A. list monitor

B. oneshot

C. btprobe

D. tailingprocessor

Correct Answer: B

QUESTION 4

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.

Correct Answer: C

QUESTION 5

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?

A. Script

B. Batch

C. Monitor

D. Fschange

Correct Answer: B

Reference: https://community.splunk.com/t5/Getting-Data-In/Is-it-possible-to-have-a-Splunk-universalforwarder-read-a/td-p/172752

Latest SPLK-3003 Dumps SPLK-3003 PDF Dumps SPLK-3003 VCE Dumps