SPLK-3003Q&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.pass4itsure.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

When monitoring and forwarding events collected from a file containing unstructured textual events, what is the difference in the Splunk2Splunk payload traffic sent between a universal forwarder (UF) and indexer compared to the Splunk2Splunk payload sent between a heavy forwarder (HF) and the indexer layer? (Assume that the file is being monitored locally on the forwarder.)

A. The payload format sent from the UF versus the HF is exactly the same. The payload size is identical because they\\'re both sending 64K chunks.

B. The UF sends a stream of data containing one set of medata fields to represent the entire stream, whereas the HF sends individual events, each with their own metadata fields attached, resulting in a lager payload.

C. The UF will generally send the payload in the same format, but only when the sourcetype is specified in the inputs.conf and EVENT_BREAKER_ENABLE is set to true.

D. The HF sends a stream of 64K TCP chunks with one set of metadata fields attached to represent the entire stream, whereas the UF sends individual events, each with their own metadata fields attached.

Correct Answer: B

QUESTION 2

When using SAML, where does user authentication occur?

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.

Correct Answer: A

QUESTION 3

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.

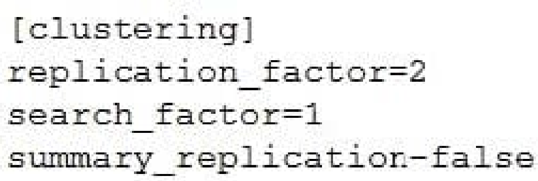
C. Edit the default user role and remove the output_file capability.

D. Clone the default user role, remove the output_file capability, and assign it to the users.

Correct Answer: C

QUESTION 4

The customer has an indexer cluster supporting a wide variety of search needs, including scheduled search, data model acceleration, and summary indexing. Here is an excerpt from the cluster mater\\'s server.conf:



```
[clustering]
replication_factor=2
search_factor=1
summary_replication-false
```

Which strategy represents the minimum and least disruptive change necessary to protect the searchability of the indexer cluster in case of indexer failure?

A. Enable maintenance mode on the CM to prevent excessive fix-up and bring the failed indexer back online.

B. Leave replication_factor=2, increase search_factor=2 and enable summary_replication.

C. Convert the cluster to multi-site and modify the server.conf to be site_replication_factor=2, site_search_factor=2.

D. Increase replication_factor=3, search_factor=2 to protect the data, and allow there to always be a searchable copy.

Correct Answer: D

QUESTION 5

The data in Splunk is now subject to auditing and compliance controls. A customer would like to ensure that at least one year of logs are retained for both Windows and Firewall events. What data retention controls must be configured?

A. maxTotalDataSizeMB and frozenTimePeriodInSecs

B. coldToFrozenDir and coldToFrozenScript

C. Splunk Volume and maxTotalDataSizMB

D. Splunk Volume and frozenTimePeriodInSecs

Correct Answer: A

Reference: https://docs.splunk.com/Documentation/Splunk/8.1.0/Indexer/Setaretirementandarchivingpolicy