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.leads4pass.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

How is a remote monitor input distributed to forwarders?

A. As an app.

B. As a forward.conf file.

C. As a monitor.conf file.

D. As a forwarder monitor profile.

Correct Answer: A

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

QUESTION 2

Which setting in indexes. conf allows data retention to be controlled by time?

A. maxDaysToKeep

B. moveToFrozenAfter

C. maxDataRetentionTime

D. frozenTimePeriodlnSecs

Correct Answer: D

https://docs.splunk.com/Documentation/Splunk/latest/Indexer/Setaretirementandarchivingpolicy

QUESTION 3

Which of the following are supported options when configuring optional network inputs?

A. Metadata override, sender filtering options, network input queues (quantum queues)

B. Metadata override, sender filtering options, network input queues (memory/persistent queues)

C. Filename override, sender filtering options, network output queues (memory/persistent queues)

D. Metadata override, receiver filtering options, network input queues (memory/persistent queues)

Correct Answer: B

https://docs.splunk.com/Documentation/Splunk/latest/Data/Monitornetworkports

QUESTION 4

Which data pipeline phase is the last opportunity for defining event boundaries?

A. Input phase

B. Indexing phase

C. Parsing phase

D. Search phase

Correct Answer: C

Reference https://docs.splunk.com/Documentation/Splunk/8.2.3/Admin/Configurationparametersandthedatapipeline

QUESTION 5

Using SEDCMD in props.conf allows raw data to be modified. With the given event below, which option will mask the first three digits of the AcctID field 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