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

If an update is made to an attribute in inputs.conf on a universal forwarder, on which Splunk component would the fishbucket need to be reset in order to reindex the data?

A. Indexer

B. Forwarder

C. Search head

D. Deployment server

Correct Answer: A

"Every Splunk instance has a fishbucket index, except the lightest of hand-tuned lightweight forwarders, and if you index a lot of files it can get quite large. As any other index, you can change the retention policy to control the size via indexes.conf"

Reference https://community.splunk.com/t5/Archive/How-to-reindex-data-from-a-forwarder/td-p/93310

QUESTION 2

Which configuration files are used to transform raw data ingested by Splunk? (Choose all that apply.)

A. props.conf

B. inputs.conf

C. rawdata.conf

D. transforms.conf

Correct Answer: AD

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

---

QUESTION 3

Which of the following types of data count against the license daily quota?

A. Replicated data

B. splunkd logs

C. Summary index data

D. Windows internal logs

Correct Answer: D

QUESTION 4

After how many warnings within a rolling 30-day period will a license violation occur with an enforced Enterprise license?

A. 1

B. 3

C. 4

D. 5

Correct Answer: D

"Enterprise Trial license. If you get five or more warnings in a rolling 30 days period, you are in violation of your license. Dev/Test license. If you generate five or more warnings in a rolling 30-day period, you are in violation of your license. Developer license. If you generate five or more warnings in a rolling 30-day period, you are in violation of your license. BUT for Free license. If you get three or more warnings in a rolling 30 days period, you are in violation of your license."

Reference: https://docs.splunk.com/Documentation/Splunk/8.0.5/Admin/Aboutlicenseviolations

QUESTION 5

You update a props. conf file while Splunk is running. You do not restart Splunk and you run this command: splunk btoo1 props list --debug. What will the output be?

A. list of all the configurations on-disk that Splunk contains.

B. A verbose list of all configurations as they were when splunkd started.

C. A list of props. conf configurations as they are on-disk along with a file path from which the configuration is located

D. A list of the current running props, conf configurations along with a file path from which the configuration was made

Correct Answer: C

https://docs.splunk.com/Documentation/Splunk/8.0.1/Troubleshooting/Usebtooltotroublesh ootconfigurations

"The btool command simulates the merging process using the on-disk conf files and creates a report showing the merged settings."

"The report does not necessarily represent what\\'s loaded in memory. If a conf file change is made that requires a service restart, the btool report shows the change even though that change isn\\'t active."

QUESTION 6

An organization wants to collect Windows performance data from a set of clients, however, installing Splunk software on these clients is not allowed. What option is available to collect this data in Splunk Enterprise?

A. Use Local Windows host monitoring.

B. Use Windows Remote Inputs with WMI.

C. Use Local Windows network monitoring.

D. Use an index with an Index Data Type of Metrics.

Correct Answer: B

https://docs.splunk.com/Documentation/Splunk/8.1.0/Data/ConsiderationsfordecidinghowtomonitorWindowsdata

"The Splunk platform collects remote Windows data for indexing in one of two ways: From Splunk forwarders, Using Windows Management Instrumentation (WMI). For Splunk Cloud deployments, you must use the Splunk Universal Forwarder on a Windows machines to montior remote Windows data."

QUESTION 7

A new forwarder has been installed with a manually created deploymentclient.conf.

What is the next step to enable the communication between the forwarder and the deployment server?

A. Restart Splunk on the deployment server.

B. Enable the deployment client in Splunk Web under Forwarder Management.

C. Restart Splunk on the deployment client.

D. Wait for up to the time set in the phoneHomeIntervalInSecs setting.

Correct Answer: A

Reference: https://docs.splunk.com/Documentation/Forwarder/8.2.3/Forwarder/Configuretheuniversalforwarder

QUESTION 8

Which of the following configuration files are used with a universal forwarder? (Choose all that apply.)

A. inputs.conf

B. monitor.conf

C. outputs.conf

D. forwarder.conf

Correct Answer: AC

Reference:

https://docs.splunk.com/Documentation/Forwarder/8.0.5/Forwarder/ Configuretheuniversalforwarder

QUESTION 9

Which of the following monitor inputs stanza headers would match all of the following files?

/var/log/www1/secure.log /var/log/www/secure.l /var/log/www/logs/secure.logs /var/log/www2/secure.log

A. [monitor:///var/log/.../secure.*]

B. [monitor:///var/log/www1/secure.*]

C. [monitor:///var/log/www1/secure.log]

D. [monitor:///var/log/www*/secure.*]

Correct Answer: C

Reference: https://docs.splunk.com/Documentation/Splunk/8.2.1/Data/Monitorfilesanddirectorieswithinputs.conf

QUESTION 10

Which Splunk indexer operating system platform is supported when sending logs from a Windows universal forwarder?

A. Any OS platform

B. Linux platform only

C. Windows platform only.

D. None of the above.

Correct Answer: A

"The forwarder/indexer relationship can be considered platform agnostic (within the sphere of supported platforms) because they exchange their data handshake (and the data, if you wish) over TCP.

QUESTION 11

Which of the following are supported configuration methods to add inputs on a forwarder? (select all that apply)

A. CLI

B. Edit inputs . conf

C. Edit forwarder.conf

D. Forwarder Management

Correct Answer: ABD

https://docs.splunk.com/Documentation/Forwarder/8.2.1/Forwarder/HowtoforwarddatatoSplunkEnterprise "You can collect data on the universal forwarder using several methods. Define inputs on the universal forwarder with the CLI. You can use the CLI to define inputs on the universal forwarder. After you define the inputs, the universal forwarder collects data based on those definitions as long as it has access to the data that you want to monitor. Define inputs on

the universal forwarder with configuration files. If the input you want to configure does not have a CLI argument for it, you can configure inputs with configuration files. Create an inputs.conf file in the directory, $SPLUNK_HOME/etc/system/local

QUESTION 12

What conf file needs to be edited to set up distributed search groups?

A. props.conf

B. search.conf

C. distsearch.conf

D. distibutedsearch.conf

Correct Answer: C

You can group your search peers to facilitate searching on a subset of them. Groups of search peers are known as "distributed search groups." You specify distributed search groups in the distsearch.conf file

Reference: https://docs.splunk.com/Documentation/Splunk/8.0.5/DistSearch/Distributedsearchgroups

QUESTION 13

After automatic load balancing is enabled on a forwarder, the time interval for switching indexers can be updated by using which of the following attributes?

A. channelTTL

B. connectionTimeout

C. autoLBFrequency

D. secsInFailureInterval

Correct Answer: C

Reference: https://docs.splunk.com/Documentation/Forwarder/8.2.1/Forwarder/Configureloadbalancing

QUESTION 14

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

A. SHOULD_LINEMERGE = true

B. BREAK_ONLY_BEFORE_DATE = true

C. BREAK_ONLY_BEFORE =

D. SHOULD_LINEMERGE = false

Correct Answer: C

Reference: https://docs.splunk.com/Documentation/SplunkCloud/latest/Data/Configureeventlinebreaking

QUESTION 15

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