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

QUESTION 1

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 2

Which of the following are methods for adding inputs in Splunk? (select all that apply)

A. CLI

B. Splunk Web

C. Editing inputs. conf

D. Editing monitor. conf

Correct Answer: ABC

https://docs.splunk.com/Documentation/Splunk/8.2.2/Data/Configureyourinputs

Add your data to Splunk Enterprise. With Splunk Enterprise, you can add data using Splunk Web or Splunk Apps. In addition to these methods, you also can use the following methods. -The Splunk Command Line Interface (CLI) -The inputs.conf configuration file. When you specify your inputs with Splunk Web or the CLI, the details are saved in a configuartion file on Splunk Enterprise indexer and heavy forwarder instances.

QUESTION 3

In a distributed environment, which Splunk component is used to distribute apps and configurations to the other Splunk instances?

A. Indexer

B. Deployer

C. Forwarder

D. Deployment server

Correct Answer: D

Reference: https://docs.splunk.com/Documentation/Splunk/8.0.5/Updating/Updateconfigurations

QUESTION 4

Which is a valid stanza for a network input?

A. [udp://172.16.10.1:9997] connection = dns sourcetype = dns

B. [any://172.16.10.1:10001] connection_host = ip sourcetype = web

C. [tcp://172.16.10.1:9997] connection_host = web sourcetype = web

D. [tcp://172.16.10.1:10001] connection_host = dns sourcetype = dns

Correct Answer: D

QUESTION 5

All search-time field extractions should be specified on which Splunk component?

A. Deployment server

B. Universal forwarder

C. Indexer

D. Search head

Correct Answer: C

Reference: https://github.com/packetiq/SplunkArchitect/blob/master/README/props.conf.spec

QUESTION 6

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 7

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 8

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 9

In which phase do indexed extractions in props.conf occur?

A. Inputs phase

B. Parsing phase

C. Indexing phase

D. Searching phase

Correct Answer: B

The following items in the phases below are listed in the order Splunk applies them (ie LINE_BREAKER occurs before TRUNCATE).

Input phase inputs.conf props.conf CHARSET NO_BINARY_CHECK CHECK_METHOD CHECK_FOR_HEADER (deprecated) PREFIX_SOURCETYPE sourcetype wmi.conf regmon-filters.conf Structured parsing phase props.conf INDEXED_EXTRACTIONS, and all other structured data header extractions Parsing phase props.conf LINE_BREAKER, TRUNCATE, SHOULD_LINEMERGE, BREAK_ONLY_BEFORE_DATE, and all other line merging settings TIME_PREFIX, TIME_FORMAT, DATETIME_CONFIG (datetime.xml), TZ, and all other time extraction settings and rules TRANSFORMS which includes per-event queue filtering, per-event index assignment, per- event routing SEDCMD MORE_THAN, LESS_THAN transforms.conf stanzas referenced by a TRANSFORMS clause in props.conf LOOKAHEAD, DEST_KEY, WRITE_META, DEFAULT_VALUE, REPEAT_MATCH

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

QUESTION 10

In case of a conflict between a whitelist and a blacklist input setting, which one is used?

A. Blacklist

B. Whitelist

C. They cancel each other out.

D. Whichever is entered into the configuration first.

Correct Answer: A

https://docs.splunk.com/Documentation/Splunk/8.0.4/Data/Whitelistorblacklistspecificincomingdat a

QUESTION 11

When are knowledge bundles distributed to search peers?

A. After a user logs in.

B. When Splunk is restarted.

C. When adding a new search peer.

D. When a distributed search is initiated.

Correct Answer: D

"The search head replicates the knowledge bundle periodically in the background or when initiating a search. " "As part of the distributed search process, the search head replicates and distributes its knowledge objects to its search peers, or indexers. Knowledge objects include saved searches, event types, and other entities used in searching accorss indexes. The search head needs to distribute this material to its search peers so that they can properly execute queries on its behalf."

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

QUESTION 12

When using license pools, volume allocations apply to which Splunk components?

A. Indexers

B. Indexes

C. Heavy Forwarders

D. Search Heads

Correct Answer: A

Reference: https://docs.splunk.com/Documentation/Splunk/8.2.3/Admin/Groups,stacks,pools,andotherterminology

QUESTION 13

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 https://docs.splunk.com/Documentation/Splunk/latest/Admin/Indexesconf https://docs.splunk.com/Documentation/Splunk/7.3.1/Admin/Indexesconf#PER_INDEX_OPTIONS

QUESTION 14

What hardware attribute would need to be changed to increase the number of simultaneous searches (ad-hoc and scheduled) on a single search head?

A. Disk

B. CPUs

C. Memory

D. Network interface cards

Correct Answer: B

https://docs.splunk.com/Documentation/Splunk/7.3.1/DistSearch/SHCarchitecture Scroll down to section titled, How the cluster handles concurrent search quotas, "Overall search quota. This quota determines the maximum number of historical searches (combined scheduled and ad hoc) that the cluster can run concurrently. This quota is configured with max_Searches_per_cpu and related settings in limits.conf."

QUESTION 15

Which Splunk configuration file is used to enable data integrity checking?

A. props.conf

B. global.conf

C. indexes.conf

D. data_integrity.conf

Correct Answer: C

Reference: https://docs.splunk.com/Documentation/Splunk/8.0.5/Security/Dataintegritycontrol