DUMPSARENA

Splunk Enterprise Certified Architect

Splunk SPLK-2002

Version Demo

Total Demo Questions: 10

Total Premium Questions: 90

Buy Premium PDF

https://dumpsarena.co

sales@dumpsarena.co

sales@dumpsarena.co
dumpsarena.co

QUESTION NO: 1

Which of the following commands is used to clear the KV store?

A. splunk clean kvstore

B. splunk clear kvstore

C. splunk delete kvstore

D. splunk reinitialize kvstore

ANSWER: A

Explanation:

Reference: https://answers.splunk.com/answers/237859/can-i-delete-all-data-from-a-kv-store-at-once.html

QUESTION NO: 2

Which of the following clarification steps should be taken if apps are not appearing on a deployment client? (Select all that apply.)

A. Check serverclass.conf of the deployment server.

B. Check deploymentclient.conf of the deployment client.

C. Check the content of SPLUNK_HOME/etc/apps of the deployment server.

D. Search for relevant events in splunkd.log of the deployment server.

ANSWER: A B C

Explanation:

Reference: https://answers.splunk.com/answers/177021/why-is-deployment-client-not-picking-up-changes-to.html

QUESTION NO: 3

Splunk configuration parameter settings can differ between multiple .conf files of the same name contained within different apps. Which of the following directories has the highest precedence?

A. System local directory.

B. System default directory.

C. App local directories, in ASCII order.

D. App default directories, in ASCII order.

ANSWER: A

Explanation:

Reference: https://docs.splunk.com/Documentation/Splunk/7.3.2/Admin/Wheretofindtheconfigurationfiles

QUESTION NO: 4

Which of the following will cause the greatest reduction in disk size requirements for a cluster of N indexers running Splunk Enterprise Security?

A. Setting the cluster search factor to N-1.

B. Increasing the number of buckets per index.

C. Decreasing the data model acceleration range.

D. Setting the cluster replication factor to N-1.

ANSWER: D

Explanation:

Reference: https://docs.splunk.com/Documentation/Splunk/7.3.2/Indexer/Systemrequirements

QUESTION NO: 5

Splunk Enterprise platform instrumentation refers to data that the Splunk Enterprise deployment logs in the _introspection index. Which of the following logs are included in this index? (Select all that apply.)

A. audit.log

B. metrics.log

C. disk_objects.log

D. resource_usage.log

ANSWER: C D

Explanation:

Reference:
https://docs.splunk.com/Documentation/Splunk/7.3.1/Troubleshooting/Abouttheplatforminstrumentationframework

QUESTION NO: 6

How does IT Service Intelligence (ITSI) impact the planning of a Splunk deployment?

A. ITSI requires a dedicated deployment server.

B. The amount of users using ITSI will not impact performance.

C. ITSI in a Splunk deployment does not require additional hardware resources.

D. Depending on the Key Performance Indicators that are being tracked, additional infrastructure may be needed.

ANSWER: D

Explanation:

Reference: https://docs.splunk.com/Documentation/ITSI/4.3.1/Install/Plan

QUESTION NO: 7

Which of the following options can improve reliability of syslog delivery to Splunk? (Select all that apply.)

A. Use TCP syslog.

B. Configure UDP inputs on each Splunk indexer to receive data directly.

C. Use a network load balancer to direct syslog traffic to active backend syslog listeners.

D. Use one or more syslog servers to persist data with a Universal Forwarder to send the data to Splunk indexers.

ANSWER: C D

QUESTION NO: 8

What log file would you search to verify if you suspect there is a problem interpreting a regular expression in a monitor stanza?

A. btool.log

B. metrics.log

C. splunkd.log

D. tailing_processor.log

ANSWER: C

Explanation:

Reference: https://answers.splunk.com/answers/479312/how-to-edit-inputsconf-to-monitor-multiple-files-w-1.html

QUESTION NO: 9

Which of the following statements describe a Search Head Cluster (SHC) captain? (Select all that apply.)

A. Is the job scheduler for the entire SHC.

B. Manages alert action suppressions (throttling).

C. Synchronizes the member list with the KV store primary.

D. Replicates the SHC's knowledge bundle to the search peers.

ANSWER: A D

Explanation:

Reference: https://docs.splunk.com/Documentation/Splunk/7.3.2/DistSearch/SHCarchitecture#role_of_the_captain

QUESTION NO: 10

A multi-site indexer cluster can be configured using which of the following? (Select all that apply.)

A. Via Splunk Web.

B. Directly edit SPLUNK_HOME/etc/system/local/server.conf

C. Run a splunk edit cluster-config command from the CLI.

D. Directly edit SPLUNK_HOME/etc/system/default/server.conf

ANSWER: A B

Explanation:

Reference: https://docs.splunk.com/Documentation/Splunk/7.3.2/Indexer/Enableclustersindetail