DUMPSARENA

Splunk Enterprise Certified Admin

Splunk SPLK-1003

Version Demo

Total Demo Questions: 10

Total Premium Questions: 137

Buy Premium PDF

https://dumpsarena.co

sales@dumpsarena.co

sales@dumpsarena.co
dumpsarena.co

QUESTION NO: 1

Where can scripts for scripted inputs reside on the host file system? (Choose all that apply.)

A. $SPLUNK_HOME/bin/scripts

B. $SPLUNK_HOME/etc/apps/bin

C. $SPLUNK_HOME/etc/system/bin

D. $SPLUNK_HOME/etc/apps//bin

ANSWER: A C D

Explanation:

Reference:
https://docs.splunk.com/Documentation/Splunk/7.3.1/Data/Getdatafromscriptedinputs#Where_to_place_the_scripts_for_scripted_inputs

QUESTION NO: 2

Which layers are involved in Splunk configuration file layering? (Choose all that apply.)

A. App context

B. User context

C. Global context

D. Forwarder context

ANSWER: A B C

QUESTION NO: 3

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

ANSWER: A C

Explanation:

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

QUESTION NO: 4

Which artifact is required in the request header when creating an HTTP event?

A. ackID

B. Token

C. Manifest

D. Host name

ANSWER: B

Explanation:

Reference: https://docs.splunk.com/Documentation/Splunk/8.2.3/Data/FormateventsforHTTPEventCollector

QUESTION NO: 5

Which Splunk component requires a Forwarder license?

A. Search head

B. Heavy forwarder

C. Heaviest forwarder

D. Universal forwarder

ANSWER: B

Explanation:

Reference: https://answers.splunk.com/answers/70017/heavy-forwarder-costs-and-licenses.html

QUESTION NO: 6

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

A. CLI

B. Edit inputs.conf

C. Edit forwarder.conf

D. Forwarder Management

ANSWER: A B

Explanation:

Reference: https://docs.splunk.com/Documentation/Forwarder/7.3.1/Forwarder/HowtoforwarddatatoSplunkEnterprise#Define_inputs_on_the_universal_forwarder_with_configuration_files

QUESTION NO: 7

Which of the following indexes come pre-configured with Splunk Enterprise? (Choose all that apply.)

A. _licence

B. _internal

C. _external

D. _thefishbucket

ANSWER: B

Explanation:

Reference: https://docs.splunk.com/Documentation/Splunk/7.3.1/Indexer/Howindexingworks

QUESTION NO: 8

Which of the following Splunk components require a separate installation package?

A. Deployment server

B. License master

C. Universal forwarder

D. Heavy forwarder

ANSWER: C

Explanation:

Reference: https://github.com/packetiq/SplunkArchitect/blob/master/Install-and-Configure-Splunk-Enterprise-Components.md

QUESTION NO: 9

Which valid bucket types are searchable? (Choose all that apply.)

A. Hot buckets

B. Cold buckets

C. Warm buckets

D. Frozen buckets

ANSWER: A B C

Explanation:

Reference: https://docs.splunk.com/Documentation/Splunk/7.3.1/Indexer/HowSplunkstoresindexes

QUESTION NO: 10

Which of the following statements apply to directory inputs? (Choose all that apply.)

A. All discovered text files are consumed.

B. Compressed files are ignored by default.

C. Splunk recursively traverses through the directory structure.

D. When adding new log files to a monitored directory, the forwarder must be restarted to take them into account.

ANSWER: C

Explanation:

Reference: https://answers.splunk.com/answers/133875/recursive-monitoring-of-directories.html