Splunk

Exam Questions SPLK-1003

Splunk Enterprise Certified Admin

NEW QUESTION 1
The universal forwarder has which capabilities when sending data? (Select all that apply.)

A. Sending alerts
B. Compressing data
C. Obfuscating/hiding data
D. Indexer acknowledgement

Answer: D

Explanation:
Reference: https://docs.splunk.com/Documentation/Splunk/7.3.1/Forwarding/Typesofforwarders

NEW QUESTION 2
Which forwarder type can parse data prior to forwarding?

A. Universal forwarder
B. Heaviest forwarder
C. Hyper forwarder
D. Heavy forwarder

Answer: D

Explanation:
Reference: https://docs.splunk.com/Documentation/Splunk/7.3.1/Forwarding/Typesofforwarders

NEW QUESTION 3
Which Splunk component consolidates the individual results and prepares reports in a distributed environment?

A. Indexers
B. Forwarder
C. Search head
D. Search peers

Answer: A

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

NEW QUESTION 4
Which Splunk component distributes apps and certain other configuration updates to search head cluster members?

A. Deployer
B. Cluster master
C. Deployment server
D. Search head cluster master

Answer: A

Explanation:
Reference: https://docs.splunk.com/Documentation/Splunk/7.3.1/DistSearch/PropagateSHCconfigurationchanges

NEW QUESTION 5
When configuring monitor inputs with whitelists or blacklists, what is the supported method of filtering the lists?

A. Slash notation
B. Regular expression
C. Irregular expression
D. Wildcard-only expression

Answer: B

Explanation:
Reference: https://docs.splunk.com/Documentation/Splunk/7.3.1/Updating/Filterclients

NEW QUESTION 6
How does the Monitoring Console monitor forwarders?

A. By pulling internal logs from forwarders.
B. By using the forwarder monitoring add-on.
C. With internal logs forwarded by forwarders.
D. With internal logs forwarder by deployment server.

Answer: A

NEW QUESTION 7
Which of the following enables compression for universal forwarders in outputs.conf?

A. [udpout:mysplunk_indexer11] compression=true
B. [tcpout] defaultGroup=my_indexers compressed=true
C. /opt/splunkforwarder/bin/splunk enable compression
D. [tcpount:my_indexers] server=mysplunk_indexer1:9997, mysplunk_indexer2:9997 decompression=false

Answer: B

Explanation:
Reference: https://docs.splunk.com/Documentation/Splunk/7.3.1/Admin/Outputsconf

NEW QUESTION 8
Local user accounts created in Splunk store passwords in which file?

A. $SPLUNK_HOME/etc/passwd
B. $SPLUNK_HOME/etc/authentication
C. $SPLUNK_HOME/etc/users/passwd.conf
D. $SPLUNK_HOME/etc/users/authentication.conf

Answer: A

Explanation:
Reference: https://docs.splunk.com/Documentation/Splunk/7.3.1/Admin/User-seedconf

NEW QUESTION 9
Which layers are involved in Splunk configuration file layering? (Select all that apply.)

A. App context
B. User context
C. Global context
D. Forwarder context

Answer: AC

Explanation:
Reference: https://docs.splunk.com/Documentation/Splunk/7.3.1/Admin/Wheretofindtheconfigurationfiles

NEW QUESTION 10
Which of the following are methods for adding inputs in Splunk? (Select all that apply.)

A. CLI
B. Splunk Web
C. Editing inpits.conf
D. Editing monitor.conf

Answer: AB

Explanation:
Reference: http://dev.splunk.com/view/dev -guide/SP-CAAAE3A

NEW QUESTION 10
Where are license files stored?

A. $SPLUNK_HOME/etc/secure
B. $SPLUNK_HOME/etc/system
C. $SPLUNK_HOME/etc/licenses
D. $SPLUNK_HOME/etc/apps/licenses

Answer: C

Explanation:
Reference: https://docs.splunk.com/Documentation/Splunk/7.3.1/Admin/LicenserCLIcommands

NEW QUESTION 11
Which of the following apply to how distributed search works? (Select all that apply.)

A. The search head dispatches searches to the peers.
B. The search peers pull the data from the forwarders.
C. Peers run searches in parallel and return their portion of results.
D. The search head consolidates the individual results and prepares reports.

Answer: A

Explanation:
Reference: https://docs.splunk.com/Documentation/Splunk/7.3.1/DistSearch/Whatisdistributedsearch

NEW QUESTION 15

.....

Thank You for Trying Our Product

We offer two products:

1st - We have Practice Tests Software with Actual Exam Questions

2nd - Questons and Answers in PDF Format

SPLK-1003 Practice Exam Features:

* SPLK-1003 Questions and Answers Updated Frequently

* SPLK-1003 Practice Questions Verified by Expert Senior Certified Staff

* SPLK-1003 Most Realistic Questions that Guarantee you a Pass on Your FirstTry

* SPLK-1003 Practice Test Questions in Multiple Choice Formats and Updatesfor 1 Year