Splunk

Exam Questions SPLK-1003

Splunk Enterprise Certified Admin

NEW QUESTION 1
In which Splunk configuration is the SEDCMD used?

A. props.conf
B. inputs.conf
C. indexes.conf
D. transforms.conf

Answer: A

Explanation:
Reference: https://answers.splunk.com/answers/212128/why-sedcmd-configured-in-propsconf-is-working-duri.html

NEW QUESTION 2
Where should apps be located on the deployment server that the clients pull from?

A. $SPLUNK_HOME/etc/apps
B. $SPLUNK_HOME/etc/search
C. $SPLUNK_HOME/etc/master-apps
D. $SPLUNK_HOME/etc/deployment-apps

Answer: A

Explanation:
Reference: https://answers.splunk.com/answers/371099/how-to-configure-deployment-apps-to-push-to-client.html

NEW QUESTION 3
What is required when adding a native user to Splunk? (Select all that apply.)

A. Password
B. Username
C. Full Name
D. Default app

Answer: CD

Explanation:
Reference: https://docs.splunk.com/Documentation/Splunk/7.3.1/Security/Addandeditusers

NEW QUESTION 4
Which Splunk forwarder type allows parsing of data before forwarding to an indexer?

A. Universal forwarder
B. Parsing forwarder
C. Heavy forwarder
D. Advanced forwarder

Answer: C

Explanation:
Reference: https://docs.splunk.com/Documentation/SplunkCloud/7.2.6/Forwarding/Typesofforwarders

NEW QUESTION 5
Which of the following are supported options when configuring optional network inputs?

A. Metadata override, sender filtering options, network input queues (quantum queues)
B. Metadata override, sender filtering options, network input queues (memory/persistent queues)
C. Filename override, sender filtering options, network output queues (memory/persistent queues)
D. Metadata override, receiver filtering options, network input queues (memory/persistent queues)

Answer: D

NEW QUESTION 6
What is the default character encoding used by Splunk during the input phase?

A. UTF-8
B. UTF-16
C. EBCDIC
D. ISO 8859

Answer: A

Explanation:
Reference: https://docs.splunk.com/Documentation/Splunk/7.3.1/Data/Configurecharactersetencoding

NEW QUESTION 7
User role inheritance allows what to be inherited from the parent role? (Select all that apply.)

A. Parents
B. Capabilities
C. Index access
D. Search history

Answer: B

Explanation:
Reference: https://docs.splunk.com/Documentation/Splunk/7.3.1/Security/Aboutusersandroles#How_users_inherit_capabilities

NEW QUESTION 8
Which of the following statements apply to directory inputs? (Select 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

NEW QUESTION 9
How would you configure your distsearch.conf to allow you to run the search below?
sourcetype=access_combined status=200 action=purchase splunk_server_group=HOUSTON

A. [distributedSearch:NYC] default = false servers = nyc1:8089, nyc2:8089 [distributedSearch:HOUSTON] default = falseservers = houston1:8089, houston2:8089
B. [distributedSearch] servers =nyc1, nyc2, houston1, houston2 [distributedSearch:NYC] default = false servers = nyc1, nyc2 [distributedSearch:HOUSTON]default = false servers = houston1, houston2
C. [distributedSearch] servers =nyc1:8089, nyc2:8089, houston1:8089, houston2:8089[distributedSearch:NYC] default= false servers = nyc1:8089, nyc2:8089 [distributedSearch:HOUSTON]default = falseservers = houston1:8089, houston2:8089
D. [distributedSearch] servers =nyc1:8089; nyc2:8089; houston1:8089; houston2:8089[distributedSearch:NYC]default = false servers = nyc1:8089; nyc2:8089 [distributedSearch:HOUSTON] default = false servers = houston1:8089; houston2:8089

Answer: D

NEW QUESTION 10
Which of the following is a valid distributed search group?

A. [distributedSearch:Paris] default = false servers = server1, server2
B. [searchGroup:Paris] default = false servers = server1:8089, server2:8089
C. [searchGroup:Paris] default = false servers = server1:9997, server2:9997
D. [distributedSearch:Paris] default = false servers = server1:8089; server2:8089

Answer: D

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

NEW QUESTION 10
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 11
Which option accurately describes the purpose of the HTTP Event Collector (HEC)?

A. A token-based HTTP input that is secure and scalable and that requires the use of forwarders.
B. A token-based HTTP input that is secure and scalable and that does not require the use of forwarders.
C. An agent-based HTTP input that is secure and scalable and that does not require the use of forwarders.
D. A token-based HTTP input that is insecure and non-scalable and that does not require the use of forwarders.

Answer: B

Explanation:

Reference: http://dev.splunk.com/view/event-collector/SP-CAAAE6M

NEW QUESTION 13
What type of data is counted against the Enterprise license at a fixed 150 bytes per event?

A. License data
B. Metrics data
C. Internal Splunk data
D. Internal Windows logs

Answer: B

Explanation:
Reference: https://answers.splunk.com/answers/581441/how-is-the-splunk-license-measured.html

NEW QUESTION 14
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.

Answer: C

NEW QUESTION 16
How often does Splunk recheck the LDAP server?

A. Every 5 minutes.
B. Each time a user logs in.
C. Each time Splunk is restarted.
D. Varies based on LDAP_refresh setting.

Answer: D

Explanation:
Reference: http://docshare02.docshare.tips/files/22651/226514302.pdf

NEW QUESTION 19
In which scenario would a Splunk Administrator want to enable data integrity check when creating an index?

A. To ensure that hot buckets are still open for writers and have not been forced to roll to a cold state.
B. To ensure that configuration files have not been tampered with for auditing and/or legal purposes.
C. To ensure that user passwords have not been tampered with for auditing and/or legal purposes.
D. To ensure that data has not been tampered with for auditing and/or legal purposes.

Answer: D

Explanation:
Reference: https://www.splunk.com/blog/2015/10/28/data-integrity-is-back-baby.html

NEW QUESTION 21
In this sourcetype definition the MAX_TIMESTAMP_LOOKAHEAD is missing. Which value would fit best?
[sshd_syslog] TIME_PREFIX = ^
TIME_FORMAT = %Y-%m-%d %H:%M:%S.%3N %z
LINE_BREAKER = ([\r\n]+)\d{4}-\d{2}-\d{2} \d{2}:\d{2}:\d{2} SHOUD_LINEMERGE = false
TRUNCATE = 0
Event example: 2018-04-13 13:42:41.214 -0500 server sshd[26219]: Connection from 172.0.2.60 port 47366

A. MAX_TIMESTAMP_LOOKAHEAD = 5
B. MAX_TIMESTAMP_LOOKAHEAD = 10
C. MAX_TIMESTAMP_LOOKAHEAD = 20
D. MAX_TIMESTAMP_LOOKAHEAD = 30

Answer: B

NEW QUESTION 26
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 31
What hardware attribute would you 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

Answer: B

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

NEW QUESTION 32
.....

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