Exam Questions SPLK-1003

Splunk Enterprise Certified Admin

https://www.2passeasy.com/dumps/SPLK-1003/

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
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 3
Which of the following are supported configuration methods to add inputs on a forwarder? (Select all that apply.)

A. CLI
B. Edit inputs.conf
C. Edit forwarder.conf
D. Forwarder Management

Answer: B

Explanation:
Reference: https://docs.splunk.com/Documentation/Forwarder/7.3.1/Forwarder/Configuretheuniversalforwarder

NEW QUESTION 4
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 5
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 6
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 7
When running the command shown below, what is the default path in which deploymentserver.conf is created?
splunk set deploy-poll deployServer:port

A. SPLUNK_HOME/etc/deployment
B. SPLUNK_HOME/etc/system/local
C. SPLUNK_HOME/etc/system/default
D. SPLUNK_HOME/etc/apps/deployment

Answer: B

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

NEW QUESTION 8
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 9
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 10
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

NEW QUESTION 10
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 11
Which of the following statements describe deployment management? (Select all that apply.)

A. Requires an Enterprise license.
B. Is responsible for sending apps to forwarders.
C. Once used, is the only way to manage forwarders.
D. Can automatically restart the host OS running the forwarder.

Answer: A

NEW QUESTION 14
What is the correct order of steps in Duo Multifactor Authentication?

A. * 1. Request Login* 2. Connect to SAML server* 3. Duo MFA* 4. Create User session* 5. Authentication Granted* 6. Log into Splunk
B. * 1. Request Login* 2. Duo MFA* 3. Authentication Granted* 4. Connect to SAML server* 5. Log into Splunk* 6. Create User session
C. * 1. Request Login* 2. Check authentication / group mapping* 3. Authentication Granted* 4. Duo MFA* 5. Create User session* 6. Log into Splunk
D. * 1. Request Login* 2. Duo MFA* 3. Check authentication / group mapping* 4. Create User session* 5. Authentication Granted* 6. Log into Splunk

Answer: C

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

NEW QUESTION 17
Where can scripts for scripted inputs reside on the host file system? (Select 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/<your_app>/bin

Answer: ACD

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

NEW QUESTION 19
What options are available when creating custom roles? (Select all that apply.)

A. Restrict search terms.
B. Whitelist search terms.
C. Limit the number of concurrent search jobs.
D. Allow or restrict indexes that can be searched.

Answer: AD

Explanation:
Reference: https://docs.splunk.com/Documentation/Splunk/7.2.6/Security/Aboutusersandroles

NEW QUESTION 24
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 29
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 34
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 35
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 39
For single line event sourcetypes, it is most efficient to set SHOULD_LINEMERGE
to what value?

A. True
B. False
C. <regex string>
D. Newline Character

Answer: B

Explanation:
Reference: https://answers.splunk.com/answers/704533/what-are-the-best-practices-for-defining-source-ty.html

NEW QUESTION 41
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 45
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 47
What is the difference between the two wildcards ... and * for the monitor stanza in inputs.conf?

A. ... is not supported in monitor stanzas.
B. There is no difference, they are interchangeable and match anything beyond directory boundaries.
C. * matches anything in that specific directory path segment, whereas ... recurses through subdirectories as well.
D. ... matches anything in that specific directory path segment, whereas * recurses through subdirectories as well.

Answer: C

Explanation:
Reference: https://docs.splunk.com/Documentation/Splunk/7.3.0/Data/Specifyinputpathswithwildcards

NEW QUESTION 51
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 55
What are the required stanza attributes when configuring the transforms.conf to manipulate or remove events?

A. REGEX, DEST, FORMAT
B. REGEX, SRC_KEY, FORMAT
C. REGEX, DEST_KEY, FORMAT
D. REGEX, DEST_KEY, FORMATTING

Answer: C

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

NEW QUESTION 58
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

Answer: D

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

NEW QUESTION 60
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 65
......