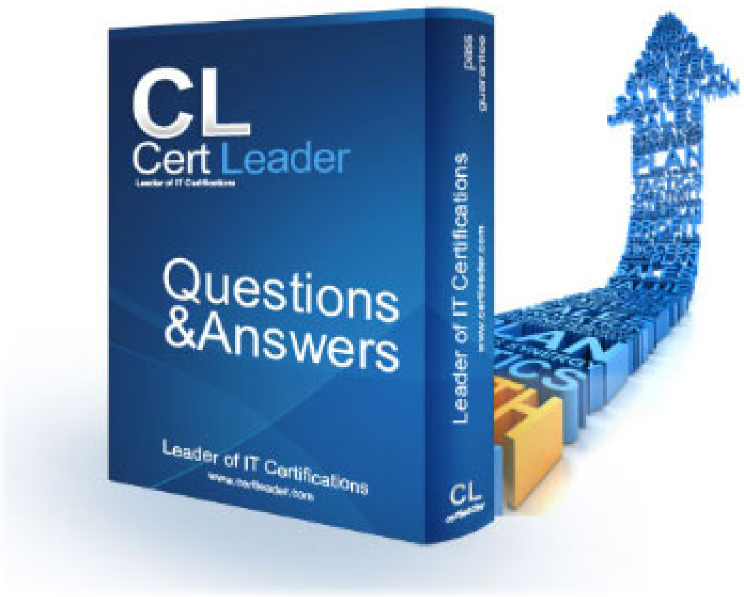
SPLK-1003 Dumps

Splunk Enterprise Certified Admin

https://www.certleader.com/SPLK-1003-dumps.html



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 parent directory contains the configuration files in Splunk?

A. $SPLUNK_HOME/etc
B. $SPLUNK_HOME/var
C. $SPLUNK_HOME/conf
D. $SPLUNK_HOME/default

Answer: A

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

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
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 7
The priority of layered Splunk configuration files depends on the file's:

A. Owner
B. Weight
C. Context
D. Creation time

Answer: C

Explanation:
Reference: https://docs.splunk.com/Documentation/Splunk/7.3.0/Admin/Wheretofindtheconfigurationfiles

NEW QUESTION 8
What are the minimum required settings when creating a network input in Splunk?

A. Protocol, port number
B. Protocol, port, location
C. Protocol, username, port
D. Protocol, IP, port number

Answer: A

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

NEW QUESTION 9
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 optional configuration setting in inputs.conf allows you to selectively forward the data to specific indexer(s)?

A. _TCP_ROUTING
B. _INDEXER_LIST
C. _INDEXER_GROUP
D. _INDEXER_ROUTING

Answer: A

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

NEW QUESTION 10
To set up a network input in Splunk, what needs to be specified?

A. File path.
B. Username and password.
C. Network protocol and port number.
D. Network protocol and MAC address.

Answer: A

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

NEW QUESTION 11
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 12
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
During search time, which directory of configuration files has the highest precedence?

A. $SPLUNK_HOME/etc/system/local
B. $SPLUNK_HOME/etc/system/default
C. $SPLUNK_HOME/etc/apps/app1/local
D. $SPLUNK_HOME/etc/users/admin/local

Answer: C

Explanation:
Reference: https://docs.splunk.com/Documentation/Splunk/7.3.0/Admin/Wheretofindtheconfigurationfiles

NEW QUESTION 17
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 22
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 24
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 27
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 32
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 33
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 34
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 38
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 41
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 45
Which of the following indexes come pre-configured with Splunk Enterprise? (Select 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

NEW QUESTION 50
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 54
Which Splunk component performs indexing and responds to search requests from the search head?

A. Forwarder
B. Search peer
C. License master
D. Search head cluster

Answer: B

Explanation:
Reference: https://www.edureka.co/blog/splunk-architecture/

NEW QUESTION 58
When deploying apps, which attribute in the forwarder management interface determines the apps that clients install?

A. App Class
B. Client Class
C. Server Class
D. Forwarder Class

Answer: C

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

NEW QUESTION 63
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 67
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 68
With authentication methods are natively supported within Splunk Enterprise? (Select all that apply.)

A. LDAP

B. SAML
C. RADIUS
D. Duo Multifactor Authentication

Answer: AD

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

NEW QUESTION 71
......