ATMIC NETWORKS
YOUR GUIDE TO GLOBAL CERTIFIATION

"Please note that these files may not be up to date. However, the questions will help you understand the exam format and typical question patterns."

www.atmicnetworks .com

Warning: Keep connected with our support team for latest updates

www.atmicnetworks.com

Question: 1

Which setting in indexes. conf allows data retention to be controlled by time?

A. maxDaysToKeep
B. moveToFrozenAfter
C. maxDataRetentionTime
D. frozenTimePeriodInSecs

Answer: D

Question: 2

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: B,D

Question: 3

In case of a conflict between a whitelist and a blacklist input setting, which one is used?

A. Blacklist
B. Whitelist
C. They cancel each other out.
D. Whichever is entered into the configuration first.

Answer: A

Question: 4

In which Splunk configuration is the SEDCMD used?

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

Answer: A

Question: 5

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: A,B,D

Question: 6

Which parent directory contains the configuration files in Splunk?

A. SSFLUNK_HOME/etc
B. SSPLUNK_HOME/var
C. SSPLUNK_HOME/conf
D. SSPLUNK_HOME/default

Answer: A

Question: 7

Which forwarder type can parse data prior to forwarding?

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

Answer: D

Question: 8

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: C

Question: 9

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: C

Question: 10

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

A. $SFLUNK_KOME/etc/apps
B. $SPLUNK_HCME/etc/sear:ch
C. $SPLUNK_HCME/etc/master-apps
D. $SPLUNK HCME/etc/deployment-apps

Answer: D

Question: 11

This file has been manually created on a universal forwarder

opt.' splunkfor warder/ et c' app * / ny_ - A/ local /inputs, conf

'monitor; / '/vac/ Log.'messages^

sour o=type= ays It g

index=syslog

A new Splunk admin comes in and connects the universal forwarders to a deployment server and deploys the same app with a new

inputs .conf file

□pt Eplunk/etc deplorett-acts/ny_TA.-''Local inputs.conf

^monitor: var leg nail Log'

s ou r cat yp e=ma illog

indexFsyslog

Which file is now monitored?

A. /var/log/messages
B. /var/log/maillog
C. /var/log/maillog and /var/log/messages
D. none of the above

Answer: B

Question: 12

In which phase of the index time process does the license metering occur?

A. input phase
B. Parsing phase
C. Indexing phase
D. Licensing phase

Answer: C

Question: 13

You update a props. conf file while Splunk is running. You do not restart Splunk and you run this command: splunk btoo1 props list —debug. What will the output be?

A. list of all the configurations on-disk that Splunk contains.
B. A verbose list of all configurations as they were when splunkd started.
C. A list of props. conf configurations as they are on-disk along with a file path from which the configuration is located
D. A list of the current running props, conf configurations along with a file path from which the configuration was made

Answer: C

Question: 14

When running the command shown below, what is the default path in which deployment server. conf is created?

splunk set deploy-poll deployServer:port

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

Answer: C

Question: 15

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

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

Answer: C

Question: 16

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

Question: 17

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: A,B

Question: 18

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

Question: 19

Which Splunk component requires a Forwarder license?

A. Search head
B. Heavy forwarder
C. Heaviest forwarder
D. Universal forwarder

Answer: B

Question: 20

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

Question: 21

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: C

Question: 22

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

Question: 23

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,B

Question: 24

During search time, which directory of configuration files has the highest precedence?

A. $SFLUNK_KOME/etc/system/local
B. $SPLUNK_KCME/etc/system/default
C. $SPLUNK_HCME/etc/apps/app1/local
D. $SPLUNK HCME/etc/users/admin/local

Answer: D

Question: 25

Within props. conf, which stanzas are valid for data modification? (select all that apply)

A. Host
B. Server
C. Source
D. Sourcetype

Answer: A,C,D

Question: 26

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

A. 1 Request Login2. Connect to SAML server3 Duo MFA4 Create User session5 Authentication Granted 6. Log into Splunk

B. 1. Request Login 2 Duo MFA3. Authentication Granted 4 Connect to SAML server5. Log into Splunk6. Create User session

C. 1 Request Login2 Check authentication / group mapping3 Authentication Granted4. Duo MFA5. Create User session6. Log into Splunk

D. 1 Request Login 2 Duo MFA3. Check authentication / group mapping4 Create User session5. Authentication Granted6 Log into Splunk

Answer: C

Question: 27

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

A. $SFLUNK_HOME/bin/scripts
B. $SPLUNK_HOME/etc/apps/bin
C. $SPLUNK_HOME/etc/system/bin
D. $S?LUNK_HOME/etc/apps/<your_app>/bin_

Answer: A,C,D

Question: 28

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 forwarded by deployment server.

Answer: C

Question: 29

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: A,C,D

Question: 30

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: B

Question: 31

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

Question: 32

Which of the following enables compression for universal forwarders in outputs. conf A)

[udp DU t: mysp 1 unk _inde xe r 1;
c cmp rosso on=0 r LIE

B)

[tcpout]
def a ill tG r oup =ny_ on dexer s
cmpzessed=true

C)

/opt/splunkforwarder/bin/splunk enable compression

D)

[tcpout:ray_indexers 1 server^ysciunk^indexerl: ?99\ mysriunk-indexerS : ?9? dec snip re s si cr.^ fa
1 s e

A. Option A B. Option B C. Option C D. Option D

www.atmicnetworks.com

Answer: B

Question: 33

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,C

Question: 34

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: A,C

Question: 35

How would you configure your distsearch conf to allow you to run the search below?
sourcetype=access_combined status=200 action=purchase splunk_setver_group=HOUSTON

A)

```
[distributedSearch' NYC]
default = false
servers-nyc 1.8089, nyc2:8O89

[distfibutedSearch HOUSTON]
default = false
servers = houstonl 8089, houston2.8089
```

B)

[disinbutedSearch]
servers = nyd. nyc2, houstonl. houston2

[distributedSearch NYC]
default - false
servers = nyd, nyc2

[distributedSearch HOUSTON]
default = false
servers - houstonl. houston2

C)
[distributed Search]
servers = nyd 8089 iwcZ80 89, houstonl.808 9 houston2:8089

[distnbutedSearch NYC]
default " false ®
servers = nyd 8089, nyc2 8089

[distributedSearEh: HOUSTON]
default = false
servers = ho Liston 1:8 089. liouston2:8089

D)
[distributedSearch]
servers = nyd 8089; nyc2:8089; houstoni 8089 hou$ton2 8089

[distributedSearch NYC]
default = false
servers = nyd 8089; nyc2:8089

[distnbutedSearch: HOUSTON)
default = false
servers = Houston 1.8 08 9 Houston2.8 089

A. option A B. Option B C. Option C D. Option D

Answer: C

www.atmicnetworks.com

Question: 36

Which of the following is valid distribute search group?

A)

B)

[searcherour: Paris;

default = false

servers = serveri:808 9, server!:5 GES

C)

[searchGrour:Paris]

default = false

servers = serveri: 9920 server! : 991“

D)

[distributeesearch:Paris J default = false

servers = serveri:8085, server!:8089

A. option A B. Option B C. Option C D. Option D

Answer: D

Question: 37

Local user accounts created in Splunk store passwords in which file?

A. $ SFLUNK_HOME/etc/passwd
B. $ SFLUNK_HOME/etc/authentication
C. $ S?LUNK_HOME/etc/users/passwd.conf
D. $ SPLUNK HOME/etc/users/authentication.conf

Answer: A

Question: 38

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

Question: 39

Which Splunk component does a search head primarily communicate with?

A. Indexer
B. Forwarder
C. Cluster master
D. Deployment server

Answer: A

Question: 40

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: A,B,C

Question: 41

Which of the following are methods for adding inputs in Splunk? (select all that apply)

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

Answer: A,B,C

Question: 42

Which of the following authentication types requires scripting in Splunk?

A. ADFS
B. LDAP
C. SAML
D. RADIUS

Answer: D

Question: 43

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

Question: 44

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 interchangable 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

Question: 45

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

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

Answer: B

Question: 46

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

A. Hot buckets
B. Cold buckets
C. Warm buckets
D. Frozen buckets

Answer: A,B,C

Question: 47

How do you remove missing forwarders from the Monitoring Console?

A. By restarting Splunk.
B. By rescanning active forwarders.
C. By reloading the deployment server.
D. By rebuilding the forwarder asset table.

Answer: D

Question: 48

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: A

Question: 49

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

Question: 50

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

A. _license
B. _lnternal
C. _external
D. thefishbucket

Answer: B,D

Question: 51

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: B

Question: 52

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

Question: 53

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 writes 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

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

Question: 55

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

Question: 56

In this source definition the MAX_TIMESTAMP_LOOKHEAD is missing. Which value would fit best?

```
[ashd ayal^g]
TIME PREFIX *
I'lML^'XOAl = Qn-^—ed fbllz^M^t.^lti %z
'TNE BREAKER ll\r\n| i)\dU|-V!PH\d|ZJ k«H 2 H \d] 21:\d 12 i
SlIOLLJ^Ll^MLkGE = false
TRUNCATE - 0
```

Event example:

2016-04-13 13:42:41.214 -0500 server sshd 126215? : Connection from 1.2.0.2.60 port 47366

A. MAX_TIMESTAMP_L0CKAHEAD = 5
B. MAX_TIMESTAMP_LOOKAHEAD - 10
C. MAX_TIMESTAMF_LOOKHEAD = 20
D. MAX TIMESTAMP LOOKAHEAD - 30

Answer: D

Question: 57

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: A,B,D

Question: 58

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,C,D

Question: 59

What hardware attribute would 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

Question: 60

Which authentication methods are natively supported within Splunk Enterprise? (select all that apply)

A. LDAP
B. SAML
C. RADIUS
D. Duo Multifactor Authentication

Answer: A,B,C

Question: 61

Which configuration files are used to transform raw data ingested by Splunk? (Choose all that apply.)

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

Answer: A,D

Question: 62

What conf file needs to be edited to set up distributed search groups?

A. props.conf
B. search.conf
C. distsearch.conf
D. distibutedsearch.conf

Answer: C

Question: 63

After configuring a universal forwarder to communicate with an indexer, which index can be checked via the Splunk Web UI for a successful connection?

A. index=main
B. index=test
C. index=summary
D. index=_internal

Answer: D

Question: 64

Which of the following are available input methods when adding a file input in Splunk Web? (Choose all that apply.)

A. Index once.
B. Monitor interval.
C. On-demand monitor.
D. Continuously monitor.

Answer: A,D

Question: 65

Which is a valid stanza for a network input?

A. [udp://172.16.10.1:9997]connection = dnssourcetype = dns
B. [any://172.16.10.1:10001]connection_host = ipsourcetype = web
C. [tcp://172.16.10.1:9997]connection_host = websourcetype = web
D. [tcp://172.16.10.1:10001]connection_host = dnssourcetype = dns

Answer: D

Question: 66

Which additional component is required for a search head cluster?

A. Deployer
B. Cluster Master
C. Monitoring Console
D. Management Console

Answer: A

Question: 67

When are knowledge bundles distributed to search peers?

A. After a user logs in.
B. When Splunk is restarted.
C. When adding a new search peer.
D. When a distributed search is initiated.

Answer: D

Question: 68

Assume a file is being monitored and the data was incorrectly indexed to an exclusive index. The index is cleaned and now the data must be reindexed. What other index must be cleaned to reset the input checkpoint

information for that file?

A. _audit
B. _checkpoint
C. _introspection
D. thefishbucket

Answer: D

Question: 69

If an update is made to an attribute in inputs.conf on a universal forwarder, on which Splunk component would the fishbucket need to be reset in order to reindex the data?

A. Indexer
B. Forwarder
C. Search head
D. Deployment server

Answer: A

Question: 70

How can native authentication be disabled in Splunk?

A. Remove the $SPLUNK_HOME/etc/passwd file
B. Create an empty $SPLUNK_HOME/etc/passwd file
C. Set SPLUNK_AUTHENTICATION=false in splunk-launch.conf
D. Set nativeAuthentication=false in authentication.conf

Answer: B

Question: 71

The volume of data from collecting log files from 50 Linux servers and 200 Windows servers will require multiple indexers. Following best practices, which types of Splunk component instances are needed?

A. Indexers, search head, universal forwarders, license master
B. Indexers, search head, deployment server, universal forwarders
C. Indexers, search head, deployment server, license master, universal forwarder
D. Indexers, search head, deployment server, license master, universal forwarder, heavy forwarder

Answer: C

Question: 72

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

Question: 73

On the deployment server, administrators can map clients to server classes using client filters. Which of the following statements is accurate?

A. The blacklist takes precedence over the whitelist.
B. The whitelist takes precedence over the blacklist.
C. Wildcards are not supported in any client filters.
D. Machine type filters are applied before the whitelist and blacklist.

Answer: A

Question: 74

Which configuration file would be used to forward the Splunk internal logs from a search head to the indexer?

A. props.conf
B. inputs.conf
C. outputs.conf
D. collections.conf

Answer: C

Question: 75

When configuring HTTP Event Collector (HEC) input, how would one ensure the events have been indexed?

A. Enable indexer acknowledgment.
B. Enable forwarder acknowledgment.
C. splunk check-integrity -index <index name>
D. index=_internal component=ACK | stats count by host

Answer: A

Question: 76

What is the valid option for a [monitor] stanza in inputs.conf?

A. enabled
B. datasource
C. server_name
D. ignoreOlderThan

Answer: D

Question: 77

Which of the following is a benefit of distributed search?

A. Peers run search in sequence.
B. Peers run search in parallel.
C. Resilience from indexer failure.
D. Resilience from search head failure.

Answer: B

Question: 78

The CLI command splunk add forward-server indexer:<receiving-port> will create stanza(s) in which configuration file?

A. inputs.conf
B. indexes.conf
C. outputs.conf
D. servers.conf

Answer: C

Question: 79

The Splunk administrator wants to ensure data is distributed evenly amongst the indexers. To do this, he runs the following search over the last 24 hours:

index=*

What field can the administrator check to see the data distribution?

A. host
B. index
C. linecount
D. splunk_server

Answer: D

Question: 80

Social Security Numbers (PII) data is found in log events, which is against company policy. SSN format is as follows: 123-44-5678.

Which configuration file and stanza pair will mask possible SSNs in the log events?

A. props.conf[mask-SSN]REX = (?ms)^(.)\<[SSN>\d{3}-?\d{2}-?(\d{4}.*)$"FORMAT = $1<SSN>###-##- $2KEY = _raw
B. props.conf[mask-SSN]REGEX = (?ms)^(.)\<[SSN>\d{3}-?\d{2}-?(\d{4}.*)$"FORMAT = $1<SSN>###- ##- $2DEST_KEY = _raw
C. transforms.conf[mask-SSN]REX = (?ms)^(.)\<[SSN>\d{3}-?\d{2}-?(\d{4}.*)$"FORMAT = $1<SSN>###-##- $2DEST_KEY = _raw
D. transforms.conf[mask-SSN]REGEX = (?ms)^(.)\<[SSN>\d{3}-?\d{2}-?(\d{4}.*)$"FORMAT = $1<SSN>###-##- $2DEST_KEY = _raw

Answer: D

Question: 81

Where are deployment server apps mapped to clients?

A. Apps tab in forwarder management interface or clientapps.conf.
B. Clients tab in forwarder management interface or deploymentclient.conf.
C. Server Classes tab in forwarder management interface or serverclass.conf.
D. Client Applications tab in forwarder management interface or clientapps.conf.

Answer: C

Question: 82

Which Splunk configuration file is used to enable data integrity checking?

A. props.conf
B. global.conf
C. indexes.conf
D. data_integrity.conf

Answer: C

Question: 83

An admin is running the latest version of Splunk with a 500 GB license. The current daily volume of new data is 300 GB per day. To minimize license issues, what is the best way to add 10 TB of historical data to the index?

A. Buy a bigger Splunk license.
B. Add 2.5 TB each day for the next 5 days.
C. Add all 10 TB in a single 24 hour period.
D. Add 200 GB of historical data each day for 50 days.

Answer: C

Question: 84

After how many warnings within a rolling 30-day period will a license violation occur with an enforced Enterprise license?

A. 1
B. 3
C. 4
D. 5

Answer: D

Question: 85

Who provides the Application Secret, Integration, and Secret keys, as well as the API Hostname when setting up Duo for Multi-Factor Authentication in Splunk Enterprise?

A. Duo Administrator
B. LDAP Administrator
C. SAML Administrator
D. Trio Administrator

Answer: A

Question: 86

When does a warm bucket roll over to a cold bucket?

A. When Splunk is restarted.
B. When the maximum warm bucket age has been reached.
C. When the maximum warm bucket size has been reached.
D. When the maximum number of warm buckets is reached.

Answer: D

Question: 87

In a distributed environment, which Splunk component is used to distribute apps and configurations to the other Splunk instances?

A. Indexer
B. Deployer
C. Forwarder
D. Deployment server

Answer: D

Question: 88

How is a remote monitor input distributed to forwarders?

A. As an app.

B. As a forward.conf file.
C. As a monitor.conf file.
D. As a forwarder monitor profile.

Answer: A

Question: 89

How is data handled by Splunk during the input phase of the data ingestion process?

A. Data is treated as streams.
B. Data is broken up into events.
C. Data is initially written to disk.
D. Data is measured by the license meter.

Answer: A

Question: 90

Which option on the Add Data menu is most useful for testing data ingestion without creating inputs.conf?

A. Upload option
B. Forward option
C. Monitor option
D. Download option

Answer: A

Question: 91

An organization wants to collect Windows performance data from a set of clients, however, installing Splunk software on these clients is not allowed. What option is available to collect this data in Splunk Enterprise?

A. Use Local Windows host monitoring.
B. Use Windows Remote Inputs with WMI.
C. Use Local Windows network monitoring.
D. Use an index with an Index Data Type of Metrics.

Answer: B

Question: 92

Which of the following must be done to define user permissions when integrating Splunk with LDAP?

A. Map Users
B. Map Groups
C. Map LDAP Inheritance
D. Map LDAP to Active Directory

Answer: B

Question: 93

In which phase do indexed extractions in props.conf occur?

A. Inputs phase
B. Parsing phase
C. Indexing phase
D. Searching phase

Answer: B

Question: 94

Which of the following statements describes how distributed search works?

A. Forwarders pull data from the search peers.
B. Search heads store a portion of the searchable data.
C. The search head dispatches searches to the search peers.
D. Search results are replicated within the indexer cluster.

Answer: C

Question: 95

Which feature in Splunk allows Event Breaking, Timestamp extractions, and any advanced configurations found in props.conf to be validated all through the UI?

A. Apps
B. Search
C. Data preview
D. Forwarder inputs

Answer: C

Question: 96

Which of the following statements accurately describes using SSL to secure the feed from a forwarder?

A. It does not encrypt the certificate password.
B. SSL automatically compresses the feed by default.
C. It requires that the forwarder be set to compressed=true.
D. It requires that the receiver be set to compression=true.

Answer: A

Question: 97

Which feature of Splunk's role configuration can be used to aggregate multiple roles intended for groups of users?

A. Linked roles
B. Grantable roles
C. Role federation
D. Role inheritance

Answer: D

Question: 98

Which of the following is the use case for the deployment server feature of Splunk?

A. Managing distributed workloads in a Splunk environment.
B. Automating upgrades of Splunk forwarder installations on endpoints.
C. Orchestrating the operations and scale of a containerized Splunk deployment.
D. Updating configuration and distributing apps to processing components, primarily forwarders.

Answer: D

Question: 99

When running a real-time search, search results are pulled from which Splunk component?

A. Heavy forwarders and search peers
B. Heavy forwarders
C. Search heads
D. Search peers

Answer: D

Question: 100

UsingSEDCMDinprops.confallows raw data to be modified. With the given event below, which option will mask the first three digits of theAcctIDfield resulting output:[22/Oct/2018:15:50:21] VendorID=1234 Code=B AcctID=xxx5309

Event:
[22/Oct/2018:15:50:21] VendorID=1234 Code=B AcctID=xxx5309

A. SEDCMD-1acct = s/VendorID=\d{3}(\d{4})/VendorID=xxx/g
B. SEDCMD-xxxAcct = s/AcctID=\d{3}(\d{4})/AcctID=xxx/g
C. SEDCMD-1acct = s/AcctID=\d{3}(\d{4})/AcctID=\1xxx/g
D. SEDCMD-1acct = s/AcctID=\d{3}(\d{4})/AcctID=xxx\1/g

Answer: D

Question: 101

Which of the following accurately describes HTTP Event Collector indexer acknowledgement?

A. It requires a separate channel provided by the client.
B. It is configured the same as indexer acknowledgement used to protect in-flight data.
C. It can be enabled at the global setting level.
D. It stores status information on the Splunk server.

Answer: A

Question: 102

What action is required to enable forwarder management in Splunk Web?

A. Navigate to Settings > Server Settings > General Settings, and set an App server port.
B. Navigate to Settings > Forwarding and receiving, and click on Enable Forwarding.
C. Create a server class and map it to a client inSPLUNK_HOME/etc/system/local/serverclass.conf.
D. Place an app in theSPLUNK_HOME/etc/deployment-appsdirectory of the deployment server.

Answer: C

Question: 103

Which of the following is accurate regarding the input phase?

A. Breaks data into events with timestamps.
B. Applies event-level transformations.
C. Fine-tunes metadata.
D. Performs character encoding.

Answer: D

Question: 104

When indexing a data source, which fields are considered metadata?

A. source, host, time
B. time, sourcetype, source
C. host, raw, sourcetype
D. sourcetype, source, host

www.atmicnetworks.com

Answer: D

Question: 105

What is the default value ofLINE_BREAKER?

A. \r\n
B. ([\r\n]+)
C. \r+\n+
D. (\r\n+)

Answer: B

Question: 106

Which of the following monitor inputs stanza headers would match all of the following files?

/var/log/www1/secure.log
/var/log/www/secure.l
/var/log/www/logs/secure.logs
/var/log/www2/secure.log

A. [monitor:///var/log/.../secure.*
B. [monitor:///var/log/www1/secure.*]
C. [monitor:///var/log/www1/secure.log]
D. [monitor:///var/log/www*/secure.*]

Answer: C

Question: 107

What are the values forhostandindexfor[stanza1]used by Splunk during index time, given the following configuration files?

SPLUNK HOME/etc/system/local/inputs.conf:

[stanzal] host=serverl

SPLUNK HOME/etc/apps/search/lccal/inputs.conf

'stanzal]

```
host=searchsvrl index=searchinfo

SPLUNK      HOME/etc/apps/search/lccal/inputs.conf
 [stanzal]
host=unixsvrl
i ndex=uni x in f o
```

A. host=server1index=unixinfo
B. host=server1index=searchinfo
C. host=searchsvr1index=searchinfo
D. host=unixsvr1index=unixinfo

Answer: A

Question: 108

An index stores its data in buckets. Which default directories does Splunk use to store buckets? (Choose all that apply.)

A. bucketdb
B. frozendb
C. colddb
D. db

Answer: C,D

Question: 109

TheLINE_BREAKERattribute is configured in which configuration file?

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

Answer: A

Question: 110

After automatic load balancing is enabled on a forwarder, the time interval for switching indexers can be updated by using which of the following attributes?

A. channelTTL
B. connectionTimeout
C. autoLBFrequency
D. secsInFailureInterval

Answer: C

Question: 111

A log file contains 193 days worth of timestamped events. Which monitor stanza would be used to collect data 45 days old and newer from that log file?

A. followTail = -45d
B. ignore = 45d
C. includeNewerThan = -35d
D. ignoreOlderThan = 45d

Answer: D

Question: 112

After an Enterprise Trial license expires, it will automatically convert to a Free license. How many days is an Enterprise Trial license valid before this conversion occurs?

A. 90 days
B. 60 days
C. 7 days
D. 14 days

Answer: B

Question: 113

Consider a company with a Splunk distributed environment in production. The Compliance Department wants to start using Splunk; however, they want to ensure that no one can see their reports or any other knowledge objects. Which Splunk Component can be added to implement this policy for the new team?

A. Indexer
B. Deployment server
C. Universal forwarder
D. Search head

Answer: D

Question: 114

Which of the following is an appropriate description of a deployment server in a non-cluster environment?

A. Allows management of local Splunk instances, requires Enterprise license, handles job of sending configurations packaged as apps. can automatically restart remote Splunk instances.
B. Allows management of remote Splunk instances, requires Enterprise license, handles job of sending configurations, can automatically restart remote Splunk instances.
C. Allows management of remote Splunk instances, requires no license, handles job of sending configurations, can automatically restart remote Splunk instances.
D. Allows management of remote Splunk instances, requires Enterprise license, handles job of sending configurations, can manually restart remote Splunk instances.

Answer: B

Question: 115

Which Splunk forwarder has a built-in license?

A. Light forwarder
B. Heavy forwarder
C. Universal forwarder
D. Cloud forwarder

Answer: C

Question: 116

What happens when the same username exists in Splunk as well as through LDAP?

A. Splunk user is automatically deleted from authentication.conf.
B. LDAP settings take precedence.
C. Splunk settings take precedence.
D. LDAP user is automatically deleted from authentication.conf

Answer: C

Question: 117

Consider the following stanza ininputs.conf:

```
[ scr i pl.: / //opt./spl unk/etc/apps/sea rch/b i n /l i sl.er. sb]

disabled - 0

interval - 60.0

sourcetype = lister
```

What will the value of the source filed be for events generated by this scripts input?

A. /opt/splunk/ecc/apps/search/bin/liscer.sh
B. unknown
C. liscer
D. liscer.sh

Answer: A

Question: 118

Which of the following applies only to Splunk index data integrity check?

A. Lookup table
B. Summary Index
C. Raw data in the index
D. Data model acceleration

Answer: C

Question: 119

Which of the following types of data count against the license daily quota?

A. Replicated data
B. splunkd logs
C. Summary index data
D. Windows internal logs

Answer: D

Question: 120

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

www.atmicnetworks.com

Question: 121

Which default Splunk role could be assigned to provide users with the following capabilities?

Create saved searches
Edit shared objects and alerts
Not allowed to create custom roles

A. admin
B. power
C. user
D. splunk-system-role

Answer: B

Question: 122

When Splunk is integrated with LDAP, which attribute can be changed in the Splunk UI for an LDAP user?

A. Default app B. LDAP group C. Password D. Username

Answer: A

Question: 123

Using the CLI on the forwarder, how could the current forwarder to indexer configuration be viewed?

A. splunk btool server list --debug
B. splunk list forward-indexer
C. splunk list forward-server
D. splunk btool indexes list --debug

Answer: C

Question: 124

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

A. ackID
B. Token
C. Manifest
D. Host name

Answer: B

Question: 125

All search-time field extractions should be specified on which Splunk component?

A. Deployment server
B. Universal forwarder
C. Indexer
D. Search head

Answer: D

Question: 126

In addition to single, non-clustered Splunk instances, what else can the deployment server push apps to?

A. Universal forwarders
B. Splunk Cloud
C. Linux package managers
D. Windows using WMI

Answer: A

Question: 127

What is the command to reset the fishbucket for one source?

A. rm -r ~/splunkforwarder/var/lib/splunk/fishbucket
B. splunk clean eventdata -index _thefishbucket
C. splunk cmd btprobe -d SPLUNK_HOME/var/lib/splunk/fishbucket/splunk_private_db --file <source> --

reset

D. splunk btool fishbucket reset <source>

Answer: C

Question: 128

Which setting allows the configuration of Splunk to allow events to span over more than one line?

A. SHOULD_LINEMERGE = true
B. BREAK_ONLY_BEFORE_DATE = true
C. BREAK_ONLY_BEFORE = <REGEX pattern>
D. SHOULD_LINEMERGE = false

Answer: A

Question: 129

In this example, ifuseACKis set to true and themaxQueueSizeis set to 7MB, what is the size of the wait queue on this universal forwarder?

A. 21MB
B. 28MB
C. 14MB
D. 7MB

Answer: A

Question: 130

Which of the following are reasons to create separate indexes? (Choose all that apply.)

A. Different retention times.
B. Increase number of users.
C. Restrict user permissions.
D. File organization.

Answer: A,C

Question: 131

Which network input option provides durable file-system buffering of data to mitigate data loss due to network outages and splunkd restarts?

A. diskQueueSize
B. durableQueueSizeC persistentOueueSize
C. queueSize

Answer: C

Question: 132

A new forwarder has been installed with a manually createddeploymentclient.conf.

What is the next step to enable the communication between the forwarder and the deployment server?

A. Restart Splunk on the deployment server.
B. Enable the deployment client in Splunk Web under Forwarder Management.
C. Restart Splunk on the deployment client.
D. Wait for up to the time set in thephoneHomeIntervalInSecssetting.

Answer: C

Question: 133

When using a directory monitor input, specific source type can be selectively overridden using which configuration file?

A. props.conf

B. sourcetypes.conf
C. transforms.conf
D. outputs.conf

Answer: A

Question: 134

When using license pools, volume allocations apply to which Splunk components?

A. Indexers
B. Indexes
C. Heavy Forwarders
D. Search Heads

Answer: A

Question: 135

An add-on has configured field aliases for source IP address and destination IP address fields. A specific user prefers not to have those fields present in their user context. Based on the defaultprops.confbelow, whichSPLUNK_HOME/etc/users/buttercup/myTA/local/props.confstanza can be added to the user's local context to disable the field aliases?

SPLUNK HOME/etc/apps/myTA/default/props*conf
[mySourcetype]
FIELDALIAS-cim-src_ip = sourcelPAddress as src_ip
FIELDALIAS-cim-dest.-ip = destinationiPaddress as destip

A.
```
[mySourcetype]
disable FIELDALIAS-cim-src_ip
disable FIELDALIAS-cim-dest-ip
```

B.
```
[mySourcetype]
FIELDALIAS-cim-src_ip =
FIELDALIAS-cim-dest-ip =
```

C.
```
[mySourcetype]
unset FIELDALIAS-cim-src_ip
unset FIELDALIAS-cim-dest-ip
```

D.
```
[mySourcetype]
#FIELDALIAS-cim-src ip = sourcelPAddress as src ip
^FIELDALIAS-cim-dest-ip - destinationiPaddress as dost ip
```

A. Option A
B. Option B
C. Option C
D. Option D

Answer: B

Question: 136

Which forwarder is recommended by Splunk to use in a production environment?

A. Heavy forwarder
B. SSL forwarder
C. Lightweight forwarder
D. Universal forwarder

Answer: D

Question: 137

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

Question: 138

Which data pipeline phase is the last opportunity for defining event boundaries?

A. Input phase
B. Indexing phase
C. Parsing phase
D. Search phase

Answer: C

Question: 139

A company moves to a distributed architecture to meet the growing demand for the use of Splunk.
What parameter can be configured to enable automatic load balancing in the
Universal Forwarder to send data to the indexers?

A. Create one outputs . conf file for each of the server addresses in the indexing tier.
B. Configure the outputs . conf file to point to any server in the indexing tier and Splunk will configure the data to be sent to all of the indexers.
C. Splunk does not do load balancing and requires a hardware load balancer to balance traffic across the indexers.
D. Set the stanza to have a server value equal to a comma-separated list of IP addresses and indexer ports for each of the indexers in the environment.

Answer: D

Question: 140

Which of the following methods will connect a deployment client to a deployment server? (select all that apply)

A. Run $SPLUNK_ROME/bin/ splunk set deploy-poll : from the command line of the deployment client.
B. Create and edit a deploymentserver . conf file in SSPLVNE{ on the deployment server.
C. Create and edit a deploymentclient . conf file in SSPLTJNE(EOME/etc/ system/local on the deployment client.
D. Run $SPLUNK ROME/bin/spiunk set deploy-poi i : from the command line of the deployment server.

Answer: A,C

Question: 141

Running this search in a distributed environment:

On what Splunk component does the eval command get executed?

A. Heavy Forwarders
B. Universal Forwarders
C. Search peers
D. Search heads

Answer: C

Question: 142

When would the following command be used?

A. To verify' the integrity of a local index.
B. To verify the integrity of a SmartStore index.
C. To verify the integrity of a SmartStore bucket.
D. To verify the integrity of a local bucket.

Answer: D

Question: 143

In inputs. conf, which stanza would mean Splunk was only reading one local file?

A. [read://opt/log/crashlog/Jan27crash.txt]
B. [monitor::/ opt/log/crashlog/Jan27crash.txt]
C. [monitor:/// opt/log/]
D. [monitor:/// opt/log/ crashlog/Jan27crash.txt]

Answer: B

Question: 144

Which of the methods listed below supports muti-factor authentication?

A. Lightweight Directory Access Protocol (LDAP)
B. Security Assertion Markup Language (SAML)
C. Single Sign-on (SSO)
D. OpenID

Answer: B

Question: 145

A Splunk administrator has been tasked with developing a retention strategy to have frequently accessed data sets on SSD storage and to have older, less frequently accessed data on slower NAS storage. They have set a mount point for the NAS. Which parameter do they need to modify to set the path for the older, less frequently accessed data in indexes.conf?

A. homepath
B. thawedPath
C. summaryHomePath
D. colddeath

Answer: D

Question: 146

A non-clustered Splunk environment has three indexers (A,B,C) and two search heads (X, Y). During a search executed on search head X, indexer A crashes. What is Splunk's response?

A. Update the user in Splunk web informing them that the results of their search may be incomplete.
B. Repeat the search request on indexer B without informing the user.
C. Update the user in Splunk web that their results may be incomple and that Splunk will try to reexecute the search.
D. Inform the user in Splunk web that their results may be incomplete and have them attempt the search from search head Y.

Answer: A

Question: 147

What is the correct curl to send multiple events through HTTP Event Collector?

```
O curl "https://mysplunkserver.example.com:8088/services/coll error" \
    -H "Authorization: Splunk DF4S7ZE4-3G51-S5F5-H777-0284GG91PF67" \
    -d "event": "Hello World", "Hole Mundo", "Halle Welt"

O curl "https: //mysplunkserver.example. com: 8G88/sarvices/collector" \
    -H "Authorization: Splunk DF457ZE4-3G51-B5F5-H777-0284GG91PF67" \
    -d "event": "Hello World", "event": "Eola Mundo", "event": "Hallo Welt"

O curl "https://mysplunkserver.example.com:S088/services/collactor" \
    -H "Authorization: Splunk DF457ZE4-3G51-85F5-H777-0284GGS1PF67" \
    -d '{"event": "Hello World"}{"event": "Hola Mundo"} {"event": "Hallo Welt", "nested": ("keyl": "valuel"}}

O curl "https://mysplunkserver.example.com:3088/services/collector" \
     H "Authorization: Splunk DF457ZE4-3G51-85F5-H777-0284GG91PF67" \
    -d *{"event": "Hello World", "Hola Mundo", "Hallo Welt", "nested": ("keyl": "valuel")}'
```

A. Option A B. Option B C. Option C D. Option D

Answer: B

Question: 148

The following stanzas in inputs. conf are currently being used by a deployment client:

[udp: //145.175.118.177:1001

Connection_host = dns

sourcetype = syslog

Which of the following statements is true of data that is received via this input?

A. If Splunk is restarted, data will be queued and then sent when Splunk has restarted.
B. Local firewall ports do not need to be opened on the deployment client since the port is defined in inputs.conf.
C. The host value associated with data received will be the IP address that sent the data.
D. If Splunk is restarted, data may be lost.

Answer: D

Question: 149

When working with an indexer cluster, what changes with the global precedence when comparing to a standalone deployment?

A. Nothing changes.
B. The peer-apps local directory becomes the highest priority.
C. The app local directories move to second in the priority list.
D. The system default directory' becomes the highest priority.

Answer: C

Question: 150

What happens when there are conflicting settings within two or more configuration files?

A. The setting is ignored until conflict is resolved.
B. The setting for both values will be used together.
C. The setting with the lowest precedence is used.
D. The setting with the highest precedence is used.

Answer: D

Question: 151

Load balancing on a Universal Forwarder is not scaling correctly. The forwarder's outputs. and the tcpout stanza are setup correctly. What else could be the cause of this scaling issue? (select all that apply)

A. The receiving port is not properly setup to listen on the right port.
B. The inputs . conf'S _SYSZOG_ROVTING is not setup to use the right group names.
C. The DNS record used is not setup with a valid list of IP addresses.
D. The indexAndForward value is not set properly.

Answer: A,C

Question: 152

A user recently installed an application to index NCINX access logs. After configuring the application, they realize that no data is being ingested. Which configuration file do they need to edit to ingest the access logs to ensure it remains unaffected after upgrade?

A. Option A B. Option B C. Option C D. Option D

Answer: A

Question: 153

What event-processing pipelines are used to process data for indexing? (select all that apply)

A. fifo pipeline
B. Indexing pipeline
C. Parsing pipeline
D. Typing pipeline

Answer: B,C

Question: 154

In a customer managed Splunk Enterprise environment, what is the endpoint URI used to collect data?

A. services/collector
B. data/collector
C. services/inputs?raw
D. services/data/collector

Answer: A

Question: 155

When using a directory monitor input, specific source types can be selectively overridden using which configuration file?

A. sourcetypes . conf
B. trans forms . conf
C. outputs . conf
D. props . conf

Answer: D

Question: 156

A configuration file in a deployed app needs to be directly edited. Which steps would ensure a successful deployment to clients?

A. Make the change in $SPLUNK HOME/etc/dep10yment apps/$appName/10ca1/ on the deployment server, and the change will be automatically sent to the deployment clients.
B. Make the change in $SPLUNK HOME /etc/apps/$appname/local/ on any of the deployment clients, and then run the command . / splunk reload deploy-server to push that change to the deployment server.
C. Make the change in $SPLUNK HOME/etc/dep10yment apps/$appName/10ca1/ on the deployment server, and then run $SPLUNK HOME/bin/sp1unk reload deploy—server.
D. Make the change in $SPLUNK HOME/etc/apps/$appName/defau1t on the deployment server, and it will be distributed down to the clients' own local versions.

Answer: C

Question: 157

What is the correct example to redact a plain-text password from raw events?

A. in props.conf:[identity]REGEX-redact_pw = s/password=([^,|/s]+)/ ####REACTED####/g
B. in props.conf:[identity]SEDCMD-redact_pw = s/password=([^,|/s]+)/ ####REACTED####/g
C. in transforms.conf:[identity]SEDCMD-redact_pw = s/password=([^,|/s]+)/ ####REACTED####/g
D. in transforms.conf:[identity]REGEX-redact_pw = s/password=([^,|/s]+)/ ####REACTED####/g

Answer: B

Question: 158

What is an example of a proper configuration for CHARSET within props.conf?

A. [host: : server. splunk. com]CHARSET = BIG5
B. [index: :main]CHARSET = BIG5
C. [sourcetype: : son]CHARSET = BIG5
D. [source: : /var/log/ splunk]CHARSET = BIG5

Answer: A

Question: 159

A security team needs to ingest a static file for a specific incident. The log file has not been collected previously and future updates to the file must not be indexed.

Which command would meet these needs?

A. splunk add one shot / opt/ incident [data .log —index incident

B. splunk edit monitor /opt/incident/data.* —index incident
C. splunk add monitor /opt/incident/data.log —index incident
D. splunk edit oneshot [opt/ incident/data.* —index incident

Answer: A

Question: 160

In a customer managed Splunk Enterprise environment, what is the endpoint URI used to collect data?

A. services/ collector
B. services/ inputs ? raw
C. services/ data/ collector
D. data/ collector

Answer: C

Question: 161

Immediately after installation, what will a Universal Forwarder do first?

A. Automatically detect any indexers in its subnet and begin routing data.
B. Begin generating internal Splunk logs.
C. Begin reading local files on its server.
D. Send an email to the operator that the installation process has completed.

Answer: B

Question: 162

A Universal Forwarder is collecting two separate sources of data (A,B). Source A is being routed through a Heavy Forwarder and then to an indexer. Source B is being routed directly to the indexer. Both sets of data require the masking of raw text strings before being written to disk. What does the administrator need to do to ensure that the masking takes place successfully?

A. Make sure that props . conf and transforms . conf are both present on the in-dexer and the search head.
B. For source A, make sure that props . conf is in place on the indexer; and for source B, make sure transforms . conf is present on the Heavy Forwarder.
C. Make sure that props . conf and transforms . conf are both present on the Universal Forwarder.

D. Place both props . conf and transforms . conf on the Heavy Forwarder for source A, and place both props . conf and transforms . conf on the indexer for source B.

Answer: D

Question: 163

The following stanza is active in indexes.conf:

[cat_facts]

maxHotSpanSecs = 3600

frozenTimePeriodInSecs = 2630000

maxTota1DataSizeMB = 650000

All other related indexes.conf settings are default values.

If the event timestamp was 3739283 seconds ago, will it be searchable?

A. Yes, only if the bucket is still hot.
B. No, because the index will have exceeded its maximum size.
C. Yes, only if the index size is also below 650000 MB.
D. No, because the event time is greater than the retention time.

Answer: D

Question: 164

Event processing occurs at which phase of the data pipeline?

A. Search
B. Indexing
C. Parsing
D. Input

Answer: C

Question: 165

Which Splunk component would one use to perform line breaking prior to indexing?

A. Heavy Forwarder
B. Universal Forwarder
C. Search head
D. This can only be done at the indexing layer.

Answer: A

Question: 166

What is a role in Splunk? (select all that apply)

A. A classification that determines what capabilities a user has.
B. A classification that determines if a Splunk server can remotely control another Splunk server.
C. A classification that determines what functions a Splunk server controls.
D. A classification that determines what indexes a user can search.

Answer: A,D

Question: 167

What is the name of the object that stores events inside of an index?

A. Container
B. Bucket
C. Data layer
D. Indexer

Answer: B

Question: 168

What will the following inputs. conf stanza do?

[script://myscript . sh]

Interval=0

A. The script will run at the default interval of 60 seconds.
B. The script will not be run.
C. The script will be run only once for each time Splunk is restarted.
D. The script will be run. As soon as the script exits, Splunk restarts it.

Answer: C

Question: 169

Which of the following describes a Splunk deployment server?

A. A Splunk Forwarder that deploys data to multiple indexers.
B. A Splunk app installed on a Splunk Enterprise server.
C. A Splunk Enterprise server that distributes apps.
D. A server that automates the deployment of Splunk Enterprise to remote servers.

Answer: C

Question: 170

What type of Splunk license is pre-selected in a brand new Splunk installation?

A. Free license
B. Forwarder license
C. Enterprise trial license
D. Enterprise license

Answer: C

Question: 171

Given a forwarder with the following outputs.conf configuration:

[tcpout : mypartner]

Server = 145.188.183.184:9097

[tcpout : hfbank]

server = inputsl . mysplunkhfs . corp : 9997 , inputs2 . mysplunkhfs . corp : 9997

Which of the following is a true statement?

A. Data will continue to flow to hfbank if 145.1 ga. 183.184 : 9097 is unreachable.
B. Data is not encrypted to mypartner because 145.188 .183.184 : 9097 is specified by IP.
C. Data is encrypted to mypartner because 145.183.184 : 9097 is specified by IP.
D. Data will eventually stop flowing everywhere if 145.188.183.184 : 9097 is unreachable.

Answer: A

Question: 172

Syslog files are being monitored on a Heavy Forwarder.

Where would the appropriate TRANSFORMS setting be deployed to reroute logs based on the event message?

A. Heavy Forwarder
B. Indexer
C. Search head
D. Deployment server

Answer: A

Question: 173

Which Splunk component(s) would break a stream of syslog inputs into individual events? (select all that apply)

A. Universal Forwarder
B. Search head
C. Heavy Forwarder
D. Indexer

Answer: C,D

Question: 174

Which pathway represents where a network input in Splunk might be found?

A. $SPLUNK HOME/ etc/ apps/ ne two r k/ inputs.conf
B. $SPLUNK HOME/ etc/ apps/ $appName/ local / inputs.conf
C. $SPLUNK HOME/ system/ local /udp.conf
D. $SPLUNK HOME/ var/lib/ splunk/$inputName/homePath/

Answer: B

Question: 175

A Universal Forwarder has the following active stanza in inputs . conf:

[monitor: //var/log]

disabled = O

host = 460352847

An event from this input has a timestamp of 10:55. What timezone will Splunk add to the event as part of indexing?

A. Universal Coordinated Time.
B. The timezone of the search head.
C. The timezone of the indexer that indexed the event.
D. The timezone of the forwarder.

Answer: D

Question: 176

Search heads in a company's European offices need to be able to search data in their New York offices. They also need to restrict access to certain indexers. What should be configured to allow this type of action?

A. Indexer clustering
B. LDAP control
C. Distributed search
D. Search head clustering

Answer: C

Question: 177

When deploying apps on Universal Forwarders using the deployment server, what is the correct component and location of the app before it is deployed?

A. On Universal Forwarder, $SPLUNK_HOME/etc/apps
B. On Deployment Server, $SPLUNK_HOME/etc/apps
C. On Deployment Server, $SPLUNK_HOME/etc/deployment-apps
D. On Universal Forwarder, $SPLUNK_HOME/etc/deployment-apps

Answer: C

Question: 178

Windows can prevent a Splunk forwarder from reading open files. If files need to be read while they are being written to, what type of input stanza needs to be created?

A. Tail Reader

B. Upload
C. MonitorNoHandle
D. Monitor

Answer: C

Question: 179

When should the Data Preview feature be used?

A. When extracting fields for ingested data.
B. When previewing the data before searching.
C. When reviewing data on the source host.
D. When validating the parsing of data.

Answer: D

Question: 180

Which file will be matched for the following monitor stanza in inputs. conf?

[monitor: ///var/log/*/bar/*. txt]

A. /var/log/host_460352847/temp/bar/file/csv/foo.txt
B. /var/log/host_460352847/bar/foo.txt
C. /var/log/host_460352847/bar/file/foo.txt
D. /var/ log/ host_460352847/temp/bar/file/foo.txt

Answer: C

Question: 181

Which scenario is applicable given the stanzas in authentication.conf below?

[authentication]
externalTwoFactorAuthVendor = Duo
externalTwoFactorAuthSettings = duoMFA

[duoMFA]
integrationKey = aGFwcHliaXJ0aGRheU1pZGR5
secretKey = YXVzdHJhaWxpYW5Gb3JHcmVw
applicationKey = c3BsaW5raW5ndGhlcGx1bWJ1c3NpbmN1OTU
apiHostname = 466993018.duosecurity.com
failOpen = True
timeout = 60

A. If Splunk cannot connect to the multifactor authentication provider, all logins will be denied.
B. Multifactor authentication is required to log into the host operating system.
C. The secretKey does not need to be protected since multifactor authentication is turned on. D. If Splunk cannot connect to the multifactor authentication provider, authentications will be successful without completing a multifactor challenge.

Answer: D

Question: 182

Which of the following is a valid method to create a Splunk user?

A. Create a support ticket.
B. Create a user on the host operating system.
C. Splunk REST API.
D. Add the username to users. conf.

Answer: C

Question: 183

An admin oversees an environment with a 1000 GBI day license. The configuration file server.conf has strict pool quota=false set. The license is divided into the following three pools, and today's usage is shown on the right-hand column:
PoolLicense SizeToday's usage
X500 GB/day100 GB
Y350 GB/day400 GB
Z150 GB/day300 GB
Given this, which pool(s) are issued warnings?

A. All pools
B. Z only

C. None
D. Y and Z

Answer: D

Question: 184

There is a file with a vast amount of old dat

a. Which of the following inputs.conf attributes would allow an admin to monitor the file for updates without indexing the pre-existing data?

A. IgnoreOlderThan
B. allowList
C. monitor
D. followTail

Answer: D

Question: 185

An admin updates the Role to Group mapping for external authentication. How does the change affect users that are currently logged into Splunk?

A. Users will continue to operate under their previous role until the next time they log into Splunk.
B. Search is disabled until users reauthenticate.
C. Only newly created user accounts are affected by the role change.
D. The role update terminates the user's current session, and they have to log back in.

Answer: A

Question: 186

When enabling data integrity control, where does Splunk Enterprise store the hash files for each bucket?

A. Splunk Enterprise stores hash files in the logdata directory of the corresponding bucket.
B. Splunk Enterprise stores hash files in the rawdata directory of the corresponding bucket.
C. Splunk Enterprise stores hash files in the hashdata directory of the corresponding bucket.
D. Splunk Enterprise stores hash files in the metadata directory of the corresponding bucket.

Answer: B

Question: 187

Which of the following is an acceptable channel value when using the HTTP Event Collector indexer acknowledgment capability?

A. GUID
B. DNS
C. Hash Checksum
D. IP Address

Answer: A

Question: 188

What is the correct order of index time precedence?
(For each of the following, highest precedence is shown at the top and lowest precedence is shown at the bottom)

A.
B. B.
C. C.
D. D.

Answer: C

Question: 189

A Universal Forwarder is monitoring a very active syslog stream and as a result is unable to switch between destinations. How would an admin safely remediate this issue?

A. Configure and enable the LINE_BREAKER on the forwarder.
B. Configure useAck on the forwarder.
C. Configure forceTimebasedAutoLB on the forwarder.
D. Configure and enable the FVFNT BREAKER on the forwarder.

Answer: C

Question: 190

What configuration file are remote Windows Management Instrumentation inputs defined in?

A. wmi_inputs.conf
B. inputs.conf
C. None, the inputs are defined outside of Splunk.
D. wmi.conf

Answer: D

Question: 191

What action could be taken to prevent a license warning with an ingest-based license?

A. Add a new license before midnight on the indexer(s).
B. Delete the data before midnight on the indexer(s).
C. Add a new license before midnight on the license manager.
D. Delete the data before midnight on the license manager.

Answer: C

Question: 192

A user is assigned two roles with the following search filters. What is the user's applied search filter?

[rd H A]

srchFiltorSolcctinq - true

::i chi'i 11*41 - s< ut ue t ype!- '; sun AND index-main

[role_B]

s r<31» l' i 1 l e rSe 1 ec! mg — l. me

srchFiltor - sourcotype-csv

A. Option A B. Option B C. Option C D. Option D

Answer: A

Question: 193

Which of the following is true when authenticating users to Splunk using LDAP?

A. LDAP group names must match the Splunk role name defined in authorize.conf.
B. Splunk will search each LDAP strategy in the order in which they are listed in authentication.conf.
C. Splunk only supports encrypted LDAP connections.

D. LDAP will take precedence over local users with the same username as defined in etc/passwd.

Answer: B

Question: 194

Which of the following is the recommended guideline for creating a new user role?

A. Create a role that incorporates capabilities and index inheritance.
B. Create a new unique role for each unique user.
C. There are no recommended guidelines when creating new user roles.
D. Create two roles based on capabilities and indexes, then utilize inheritance.

Answer: A

Question: 195

Which of the following lists the three phases of the Splunk Indexing process in order?

A. Ingest phaseLicensing phaseParsing phase
B. Sourcetype phaseIndex phaseWrite-to-disk phase
C. Input phaseParsing phaseIndexing phase
D. Ingest phaseTransforming phaseIndexing phase

Answer: C

Question: 196

Which of the following CLI commands removes a search peer from Distributed Search?

A. splunk remove search-server -auth admin:password 123.45.67.89:8089
B. splunk clear search-server -auth admin:password 123.45.67.89:8089
C. splunk clear search-peer -auth admin:password 123.45.67.89:8089
D. splunk remove search-peer -auth admin:password 123.45.67.89:8089

Answer: A