SPLK-1003.VCEplus.premium.exam.60q

Number: SPLK-1003
Passing Score: 800
Time Limit: 120 min
File Version: 1.0

SPLK-1003

Splunk Enterprise Certified Admin

Version 1.0

Exam A

QUESTION 1

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

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

Correct Answer: D
Section: (none)
Explanation

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

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

Correct Answer: D
Section: (none)
Explanation

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

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.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Reference: https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=8&ved=2ahUKEwj0r6Lso6bkAhUqxYUKHbWlDz4QFjAHegQIAxAC&url=http%3A%2F%2Fsplunk.training%2Fshowpdf.asp%3Fdata%
3D789BB6B10C1B4376B548D711B4377F3F4B511B437805A8EC11B437742EA8F11B43779B6FA211B4376EA657C11B4376FC19B311B4377E2407E11B43730AF97411B4377F3F4B511B437742EA8F11B43779B6FA211B43771F822111
B437731365811B43730AF97411B437789BB6B11B4376B548D711B4377F3F4B511B437805A8EC11B437742EA8F11B43779B6FA211B4376EA657C11B4376FC19B311B4377E2407E11B43732E61E211B4377F3F4B511B437742EA8F11
B
43779B6FA211B43771F822111B437731365811B43746D0DC011B4377549EC611B4377BED81011B437789BB6B11B4376D8B14511B437731365811B4376B548D711B4377F3F4B511B4376FC19B311B43732E61E211B4376D8B14511B4
3
77AD23D911B437789BB6B11B43730AF97411B4373989B2C11B437386E6F511B437386E6F511B4373DF6C0811B43737532BE11B4373BC039A11B437351CA5011B43737532BE11B43730AF97411B4375BD6DD511B43730AF97411B43
7564E8C211B43730AF97411B437%257C2318D1%257C11649A&usg=AOvVaw2e9s-JweivuCkqTb4-Y9uW

QUESTION 4 In which Splunk configuration is the `SEDCMD` used?

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

Correct Answer: A
Section: (none)
Explanation

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

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

Correct Answer: B
Section: (none)
Explanation

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

QUESTION 6 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`

Correct Answer: A
Section: (none)
Explanation

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

QUESTION 7 Which forwarder type can parse data prior to forwarding?

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

Correct Answer: D
Section: (none)
Explanation

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

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

Correct Answer: A
Section: (none)
Explanation

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

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

Correct Answer: A
Section: (none)
Explanation

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

QUESTION 10 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`

Correct Answer: A
Section: (none)
Explanation

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

QUESTION 11 This file has been manually created on a universal forwarder:

```
/opt/splunkforwarder/etc/apps/my_TA/local/inputs.conf
[monitor:///var/log/messages]
sourcetype=syslog
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:

```
/opt/splunk/etc/deployment-apps/my_TA/local/inputs.conf
```

```
[monitor:///var/log/maillog]
sourcetype=maillog
index=syslog
```

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

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

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

Correct Answer: C
Section: (none)
Explanation

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

QUESTION 13
You update a `props.conf` file while Splunk is running. You do not restart Splunk and you run this command: `splunk btool props list --debug`. What will the output be?

A. 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.

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Reference: https://answers.splunk.com/answers/494219/need-help-with-what-should-be-a-simple-precedence.html

QUESTION 14
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`

Correct Answer: B
Section: (none)
Explanation

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

QUESTION 15
The priority of layered Splunk configuration files depends on the file's:

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

Correct Answer: C
Section: (none)
Explanation

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

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

Correct Answer: B
Section: (none)
Explanation

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

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

Correct Answer: CD
Section: (none)
Explanation

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

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

Correct Answer: A
Section: (none)
Explanation

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

QUESTION 19 Which Splunk component requires a Forwarder license?

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

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Reference: https://answers.splunk.com/answers/70017/heavy-forwarder-costs-and-licenses.html

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`

Correct Answer: A
Section: (none)
Explanation

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

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.

Correct Answer: A
Section: (none)
Explanation

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

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

Correct Answer: C
Section: (none)
Explanation
Explanation/Reference:
Reference: https://docs.splunk.com/Documentation/SplunkCloud/7.2.6/Forwarding/Typesofforwarders

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.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 24 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`

Correct Answer: C
Section: (none)
Explanation

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

QUESTION 25 Within `props.conf`, which stanzas are valid for data modification? (Select all that apply.)

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

Correct Answer: CD
Section: (none)
Explanation

Explanation/Reference:
Reference: https://answers.splunk.com/answers/3687/host-stanza-in-props-conf-not-being-honored-for-udp-514-data-sources.html

QUESTION 26 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 SplunkB. 1. Request Login
2. Duo MFA
3. Authentication Granted
4. Connect to SAML server
5. Log into Splunk
6. Create User sessionC. 1. Request Login
2. Check authentication / group mapping
3. Authentication Granted
4. Duo MFA
5. Create User session
6. Log into SplunkD. 1. Request Login
2. Duo MFA
3. Check authentication / group mapping
4. Create User session
5. Authentication Granted
6. Log into Splunk

Correct Answer: C
Section: (none)
Explanation

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

QUESTION 27 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`

Correct Answer: ACD
Section: (none)
Explanation

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

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 forwarder by deployment server.

Correct Answer: A

Section: (none)
Explanation

Explanation/Reference:

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.

Correct Answer: AD
Section: (none)
Explanation

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

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)

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

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

Correct Answer: A
Section: (none)
Explanation

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

QUESTION 32
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`

Correct Answer: B
Section: (none)
Explanation

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

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

Correct Answer: B
Section: (none)
Explanation

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

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.

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Reference: https://answers.splunk.com/answers/133875/recursive-monitoring-of-directories.html

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_server_group=HOUSTON

A. [distributedSearch:NYC] default =
false servers = nyc1:8089,
nyc2:8089
[distributedSearch:HOUSTON]
default = false
servers = 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 = false
servers = 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

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 36 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`

Correct Answer: D
Section: (none)
Explanation

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

QUESTION 37 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`

Correct Answer: A
Section: (none)
Explanation

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

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

Correct Answer: B
Section: (none)
Explanation

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

QUESTION 39 Which Splunk component does a search head primarily communicate with?

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

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Reference: https://docs.splunk.com/Documentation/Splunk/7.3.1/InheritedDeployment/Deploymenttopology

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

Correct Answer: AC
Section: (none)
Explanation

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

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`

Correct Answer: AB
Section: (none)
Explanation

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

QUESTION 42 Which of the following authentication types requires scripting in Splunk?

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

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Reference: https://answers.splunk.com/answers/131127/scripted-authentication.html

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.

Correct Answer: B
Section: (none)
Explanation

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

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 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.

Correct Answer: C
Section: (none)
Explanation

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

QUESTION 45 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

Correct Answer: B
Section: (none)
Explanation

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

QUESTION 46 Which valid bucket types are searchable? (Select all that apply.)

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

Correct Answer: ABC
Section: (none)
Explanation

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

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.

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Reference: https://answers.splunk.com/answers/447096/how-to-remove-missing-forwarders-from-the-distribu.html

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.

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

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

Correct Answer: C
Section: (none)
Explanation

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

QUESTION 50
Which of the following indexes come pre-configured with Splunk Enterprise? (Select all that apply.)

A. _licence
B. _internal
C. _external
D. _thefishbucket

Correct Answer: B
Section: (none)
Explanation

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

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.

Correct Answer: D
Section: (none)
Explanation

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

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`

Correct Answer: C
Section: (none)
Explanation

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

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 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.

Correct Answer: D
Section: (none)
Explanation

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

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

Correct Answer: B
Section: (none)
Explanation

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

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

Correct Answer: C
Section: (none)
Explanation

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

QUESTION 56 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`

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

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`

Correct Answer: D
Section: (none)
Explanation

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

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.

Correct Answer: A
Section: (none)
Explanation

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

QUESTION 59
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

Correct Answer: B
Section: (none)
Explanation

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

QUESTION 60 With authentication methods are natively supported within Splunk Enterprise? (Select all that apply.)

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

Correct Answer: AD
Section: (none)
Explanation

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