# Splunk

## Exam SPLK-1003

### Splunk Enterprise Certified Admin

**Version: 11.0**

**[ Total Questions: 138 ]**

## Question No : 1

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**

**Explanation:** https://docs.splunk.com/Documentation/Splunk/8.0.5/Deploy/Datapipeline "In the input segment, Splunk software consumes data. It acquires the raw data stream from its source, breaks in into 64K blocks, and annotates each block with some metadata keys."

Reference: https://docs.splunk.com/Documentation/Splunk/8.0.5/Deploy/Datapipeline

## Question No : 2

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**

**Explanation:** "You can group your search peers to facilitate searching on a subset of them. Groups of search peers are known as "distributed search groups." You specify distributed search groups in the distsearch.conf file"

Reference:
https://docs.splunk.com/Documentation/Splunk/8.0.5/DistSearch/Distributedsearchgroups

## Question No : 3

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**

**Explanation:** https://docs.splunk.com/Documentation/Splunk/latest/Deploy/Datapipeline "The data pipeline segments in depth. INPUT - In the input segment, Splunk software consumes data. It acquires the raw data stream from its source, breaks it into 64K blocks, and annotates each block with some metadata keys. The keys can also include values that are used internally, such as the character encoding of the data stream, and values that control later processing of the data, such as the index into which the events should be stored. PARSING Annotating individual events with metadata copied from the source-wide keys. Transforming event data and metadata according to regex transform rules."

## Question No : 4

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 in SPLUNK_HOME/etc/system/local/serverclass.conf.
**D.** Place an app in the SPLUNK_HOME/etc/deployment-apps directory of the deployment server.

**Answer: C**

Reference:
https://docs.splunk.com/Documentation/Splunk/8.2.1/Updating/Forwardermanagementoverview

https://docs.splunk.com/Documentation/MSApp/2.0.3/MSInfra/Setupadeploymentserver

"To activate deployment server, you must place at least one app into %SPLUNK_HOME%\etc\deployment-apps on the host you want to act as deployment server. In this case, the app is the "send to indexer" app you created earlier, and the host is the indexer you set up initially.

## Question No : 5

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 No : 6

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 No : 7

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**

**Explanation:**

https://docs.splunk.com/Documentation/Splunk/8.0.1/Troubleshooting/Usebtooltotroubleshootconfigurations

"The btool command simulates the merging process using the on-disk conf files and creates a report showing the merged settings."

"The report does not necessarily represent what's loaded in memory. If a conf file change is made that requires a service restart, the btool report shows the change even though that change isn't active."

## Question No : 8

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**

**Explanation:**

Per the provided Splunk reference URL

https://docs.splunk.com/Documentation/Splunk/8.0.5/Data/AboutHECIDXAck

"While HEC has precautions in place to prevent data loss, it's impossible to completely prevent such an occurrence, especially in the event of a network failure or hardware crash. This is where indexer acknolwedgment comes in."

Reference https://docs.splunk.com/Documentation/Splunk/8.0.5/Data/AboutHECIDXAck

## Question No : 9

Which Splunk component requires a Forwarder license?

**A.** Search head
**B.** Heavy forwarder

**C.** Heaviest forwarder
**D.** Universal forwarder

**Answer: B**

## Question No : 10

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**
Reference: https://community.splunk.com/t5/All-Apps-and-Add-ons/How-do-I-configure-a-Splunk-Forwarder-on-Linux/m-p/72078

## Question No : 11

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**
**Explanation:** http://www.splunk.com/view/SP-CAAAGPR

## Question No : 12

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**

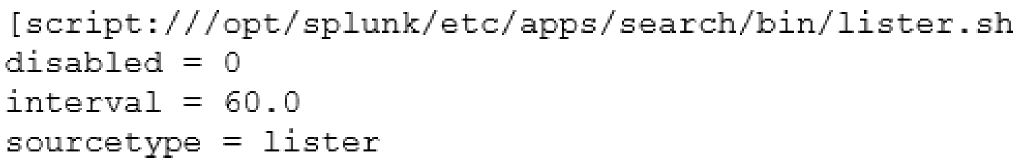
**Explanation:**

https://docs.splunk.com/Documentation/Splunk/8.0.5/Admin/Aboutlicenseviolations "Enterprise Trial license. If you get five or more warnings in a rolling 30 days period, you are in violation of your license. Dev/Test license. If you generate five or more warnings in a rolling 30-day period, you are in violation of your license. Developer license. If you generate five or more warnings in a rolling 30-day period, you are in violation of your license. BUT for Free license. If you get three or more warnings in a rolling 30 days period, you are in violation of your license."

Reference:
https://docs.splunk.com/Documentation/Splunk/8.0.5/Admin/Aboutlicenseviolations

## Question No : 13

Consider the following stanza in inputs.conf:



```
[script:///opt/splunk/etc/apps/search/bin/lister.sh
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**

**Explanation:** https://docs.splunk.com/Documentation/Splunk/8.2.2/Admin/Inputsconf

-Scroll down to source = <string>

*Default: the input file path

## Question No : 14

A new forwarder has been installed with a manually created deploymentclient.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 the phoneHomeIntervalInSecs setting.

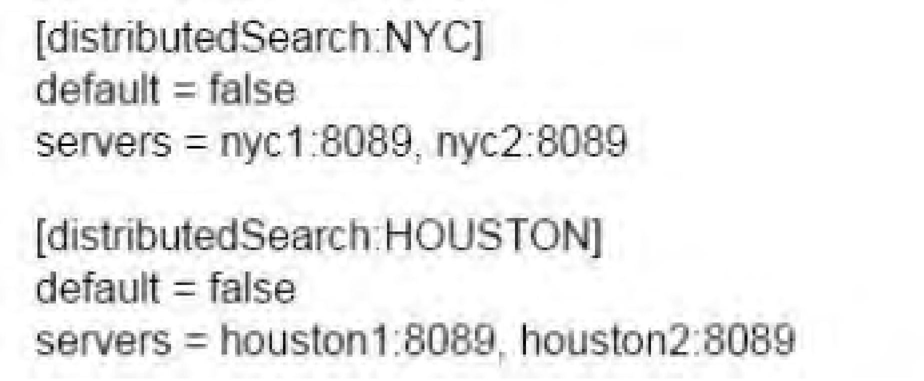
**Answer: A**

Reference:
https://docs.splunk.com/Documentation/Forwarder/8.2.3/Forwarder/Configuretheuniversalforwarder

## Question No : 15

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

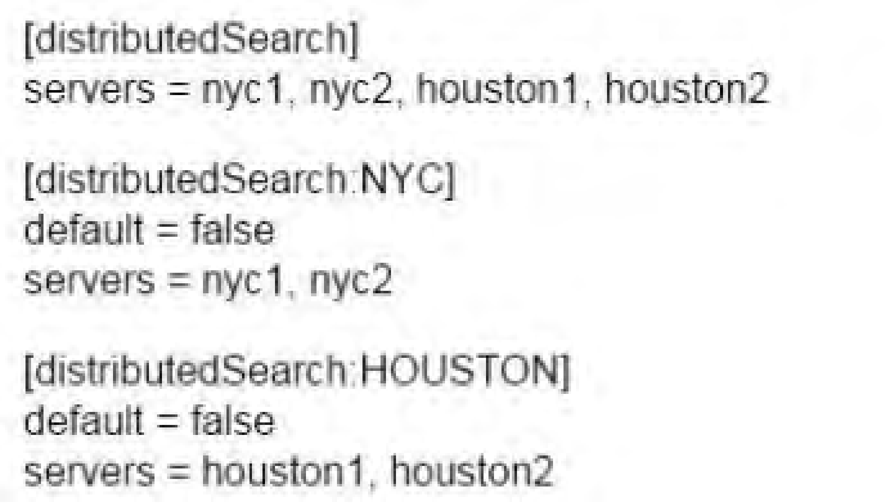
A)



```
[distributedSearch:NYC]
default = false
servers = nyc1:8089, nyc2:8089

[distributedSearch:HOUSTON]
default = false
servers = houston1:8089, houston2:8089
```

B)

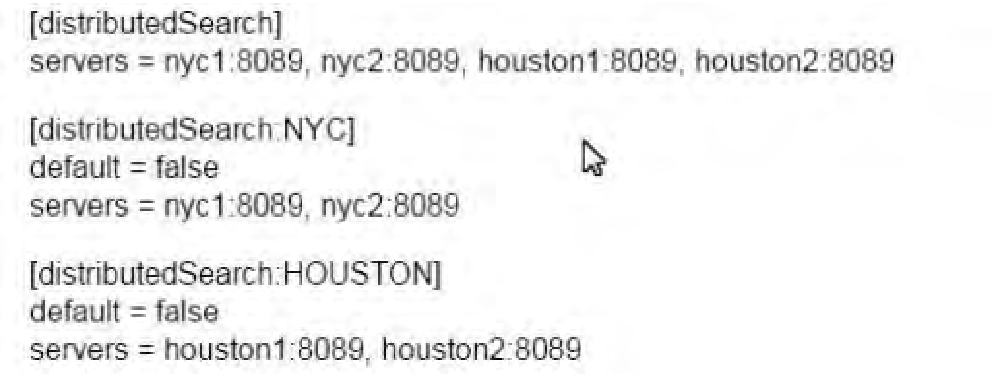


```
[distributedSearch]
servers = nyc1, nyc2, houston1, houston2

[distributedSearch:NYC]
default = false
servers = nyc1, nyc2

[distributedSearch:HOUSTON]
default = false
servers = houston1, houston2
```

C)

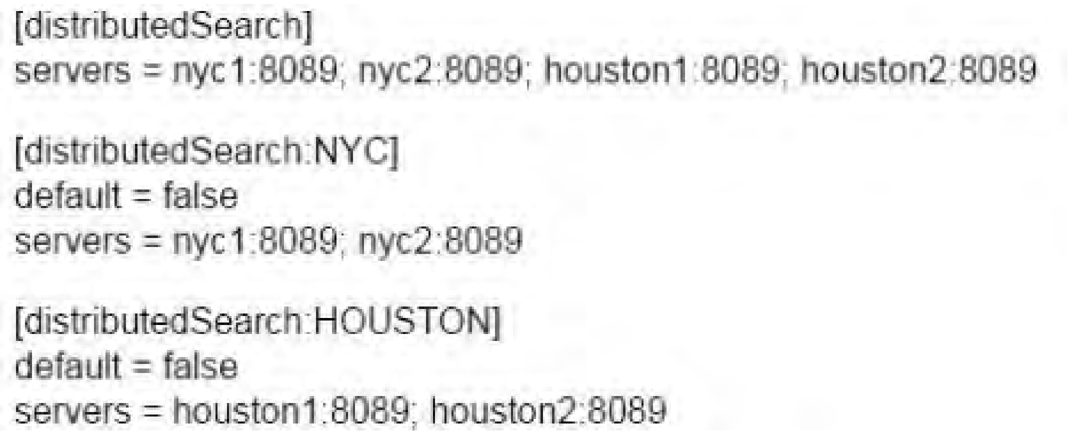


```
[distributedSearch]
servers = nyc1:8089, nyc2:8089, houston1:8089, houston2:8089

[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
```

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

**Answer: C**

**Explanation:**

https://docs.splunk.com/Documentation/Splunk/8.0.3/DistSearch/Distributedsearchgroups

**Question No : 16**

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,D**

Reference: https://community.splunk.com/t5/Getting-Data-In/Why-does-Splunk-have-multiple-indexes/m-p/12063

**Question No : 17**

Which additional component is required for a search head cluster?

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

**Answer: A**
Reference:
https://docs.splunk.com/Documentation/Splunk/8.0.5/DistSearch/SHCdeploymentoverview

The deployer. This is a Splunk Enterprise instance that distributes apps and other configurations to the cluster members. It stands outside the cluster and cannot run on the same instance as a cluster member. It can, however, under some circumstances, reside on the same instance as other Splunk Enterprise components, such as a deployment server or an indexer cluster master node.

## Question No : 18

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**
**Explanation:**
https://docs.splunk.com/Documentation/Splunk/8.1.2/Security/Dataintegritycontrol#:~:text=When%20you%20enable%20data%20integrity%20control%2C%20Splunk%20Enterprise%20computes%20hashes,it%20to%20a%20l1Hashes%20file.

Reference:
https://docs.splunk.com/Documentation/Splunk/8.0.5/Security/Dataintegritycontrol

## Question No : 19

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**

**Explanation:** https://docs.splunk.com/Documentation/Splunk/8.2.1/Updating/Filterclients

Reference: https://community.splunk.com/t5/Getting-Data-In/Can-I-use-both-the-whitelist-AND-blacklist-forthe-

same/td-p/390910

## Question No : 20

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?

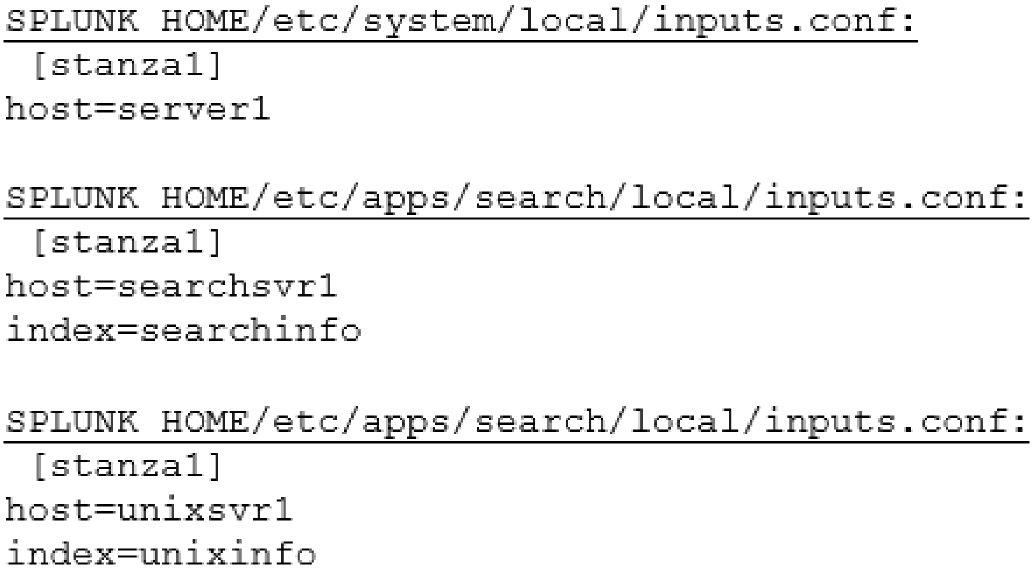
**A.** host
**B.** index
**C.** linecount
**D.** splunk_server

**Answer: D**

**Explanation:**
https://docs.splunk.com/Documentation/Splunk/8.2.2/Knowledge/Usedefaultfields
splunk_server
The splunk server field contains the name of the Splunk server containing the event. Useful in a distributed Splunk environment. Example: Restrict a search to the main index on a server named remote. splunk_server=remote index=main 404

## Question No : 21

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



```
SPLUNK HOME/etc/system/local/inputs.conf:
 [stanza1]
host=server1

SPLUNK HOME/etc/apps/search/local/inputs.conf:
 [stanza1]
host=searchsvr1
index=searchinfo

SPLUNK HOME/etc/apps/search/local/inputs.conf:
 [stanza1]
host=unixsvr1
index=unixinfo
```

**A.** host=server1
index=unixinfo
**B.** host=server1
index=searchinfo
**C.** host=searchsvr1
index=searchinfo
**D.** host=unixsvr1
index=unixinfo

**Answer: A**

**Explanation:** - etc/system/local/ has better precedence at index time - for identical settings in the same file, the last one overwrite others, see :
https://community.splunk.com/t5/Getting-Data-In/What-is-the-precedence-for-identical-stanzas-within-a-single/m-p/283566

## Question No : 22

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**

**Explanation:**

https://docs.splunk.com/Documentation/Splunk/8.0.5/Updating/Updateconfigurations First line says it all: "The deployment server distributes deployment apps to clients."

**Question No : 23**

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**

**Explanation:**

Using the Splunk reference URL https://docs.splunk.com/Splexicon:Searchpeer

"search peer is a splunk platform instance that responds to search requests from a search head. The term "search peer" is usally synonymous with the indexer role in a distributed search topology. However, other instance types also have access to indexed data, particularly internal diagnostic data, and thus function as search peers when they respond to search requests for that data."

**Question No : 24**

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

**A.** Inputs phase

**B.** Parsing phase
**C.** Indexing phase
**D.** Searching phase

**Answer: B**

**Explanation:** The following items in the phases below are listed in the order Splunk applies them (ie LINE_BREAKER occurs before TRUNCATE).

Input phase
inputs.conf
props.conf
CHARSET
NO_BINARY_CHECK
CHECK_METHOD
CHECK_FOR_HEADER (deprecated)
PREFIX_SOURCETYPE
sourcetype
wmi.conf
regmon-filters.conf
Structured parsing phase
props.conf
INDEXED_EXTRACTIONS, and all other structured data header extractions
Parsing phase
props.conf
LINE_BREAKER, TRUNCATE, SHOULD_LINEMERGE, BREAK_ONLY_BEFORE_DATE, and all other line merging settings
TIME_PREFIX, TIME_FORMAT, DATETIME_CONFIG (datetime.xml), TZ, and all other time extraction settings and rules
TRANSFORMS which includes per-event queue filtering, per-event index assignment, per-event routing
SEDCMD
MORE_THAN, LESS_THAN
transforms.conf
stanzas referenced by a TRANSFORMS clause in props.conf
LOOKAHEAD, DEST_KEY, WRITE_META, DEFAULT_VALUE, REPEAT_MATCH

Reference: https://docs.splunk.com/Documentation/Splunk/8.0.5/Admin/

Configurationparametersandthedatapipeline