Vendor: Splunk

Exam Code: SPLK-1003

Exam Name: Splunk Enterprise Certified Admin

Q&As: 182 (There are 2 parts in the dump, 182 questions in total.)

Exam A

QUESTION 1
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.

Correct Answer: C
Explanation

Explanation/Reference:
The inputs.conf file is used to configure inputs, distributed inputs such as forwarders, and file system monitoring in Splunk. The [script://myscript.sh] stanza specifies a script input, which means that Splunk runs the script and indexes its output.
The interval setting determines how often Splunk runs the script. If the interval is set to 0, the script runs only once when Splunk starts up. If the interval is omitted, the script runs at the default interval of 60 seconds. Therefore, option C is correct, and the other options are incorrect.

QUESTION 2
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.

Correct Answer: C
Explanation

Explanation/Reference:
According to the Splunk documentation, to customize a configuration file, you need to create a new file with the same name in a local or app directory. Then, add the specific settings that you want to customize to the local configuration file. Never change or copy the configuration files in the default directory. The files in the default directory must remain intact and in their original location. The Splunk Enterprise upgrade process overwrites the default directory. To deploy configuration files to deployment clients, you need to use the deployment server. The deployment server is a Splunk Enterprise instance that distributes content and updates to deployment clients. The deployment server uses a directory called $SPLUNK_HOME/etc/deployment-apps to store the apps and configuration files that itdeploys to clients. To update the configuration files in this directory, you need to edit them manually and then run the command $SPLUNK_HOME/bin/sp1unk reload deploy--server to make the changes take effect. Therefore, option A is incorrect because it does not include the reload command. Option B is incorrect because it makes the change on a deployment client instead of the deployment server. Option D is incorrect because it changes the default directory instead of the local directory.
References:
1: How to edit a configuration file - Splunk Documentation
2: Deployment of configuration files - Splunk Community

QUESTION 3
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

Correct Answer: C
Explanation

Explanation/Reference:
Reference:https://community.splunk.com/t5/All-Apps-and-Add-ons/How-do-I-configure-a- Splunk-Forwarder-on-Linux/m-p/72078
The CLI command to view the current forwarder to indexer configuration is splunk list forward-server. This command displays the hostnames and port numbers of the indexers that the forwarder sends data to. Therefore, option C is the correct answer. References: Splunk Enterprise Certified Admin | Splunk, [Use CLI commands to manage your forwarders - Splunk Documentation]

QUESTION 4
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: ACD
Explanation

Explanation/Reference:
Users log on to the search head and run reports:
The search head dispatches searches to the peers
Peers run searches in parallel and return their portion of results
The search head consolidates the individual results and prepares reports

QUESTION 5
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

Correct Answer: C
Explanation

Explanation/Reference:
https://docs.splunk.com/Documentation/Splunk/8.1.1/Updating/Definedeploymentclasses#
Ways_to_define_server_classes "When you use forwarder management to create a new server class, it saves the server class definition in a copy of serverclass.conf under $SPLUNK_HOME/etc/system/local. If, instead of using forwarder management, you decide to directly edit serverclass.conf, it is recommended that you create the serverclass.conf file in that same directory, $SPLUNK_HOME/etc/system/local."

QUESTION 6
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.

Correct Answer: AD
Explanation

Explanation/Reference:
A role in Splunk is a classification that determines what capabilities and indexes a user has.A capability is a permission to perform a specific action or access a specific feature on the Splunk platform1.An index is a collection of data that Splunk software processes and stores2. By assigning roles to users, you can control what they can do and what data they can access on the Splunk platform. Therefore, the correct answers are A and D. A role in Splunk determines what capabilities and indexes a user has. Option B is incorrect because Splunk servers do not use roles to remotely control each other.Option C is incorrect because Splunk servers use instances and components to determine what functions they control3.
References:1:Define roles on the Splunk platform with capabilities - Splunk Documentation2:About indexes and indexers - Splunk Documentation3:Splunk Enterprise components - Splunk Documentation

QUESTION 7
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: ABD
Explanation

Explanation/Reference:
homePath = $SPLUNK_DB/hatchdb/db
coldPath = $SPLUNK_DB/hatchdb/colddb
thawedPath = $SPLUNK_DB/hatchdb/thaweddb

QUESTION 8
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.

Correct Answer: C
Explanation

Explanation/Reference:
"To activate distributed search, you add search peers, or indexers, to a Splunk Enterprise instance that you desingate as a search head. You do this by specifying each search peer manually."

QUESTION 9
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.*]

Correct Answer: C
Explanation

QUESTION 10
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

Correct Answer: C
Explanation

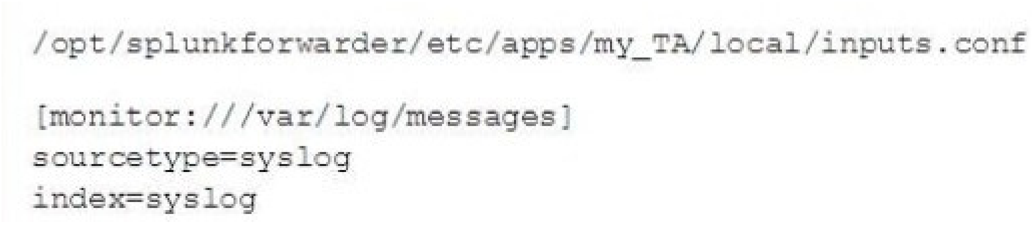
Explanation/Reference:
The correct answer is C. Distributed search is the feature that allows search heads in a company's European offices to search data in their New York offices.Distributed search also enables restricting access to certain indexers by using the splunk_server field or the server.conf file1.
Distributed search is a way to scale your Splunk deployment by separating the search management and presentation layer from the indexing and search retrieval layer. With distributed search, a Splunk instance called a search head sends search requests to a group of indexers, or search peers, which perform the actual searches on their indexes.The search head then merges the results back to the user2. Distributed search has several use cases, such as horizontal scaling, access control, and managing geo-dispersed data.For example, users in different offices can search data across the enterprise or only in their local area, depending on their needs and permissions2.
The other options are incorrect because:
A. Indexer clustering is a feature that replicates data across a group of indexers to ensure data availability and recovery.Indexer clustering does not directly affect distributed search, although search heads can be configured to search across an indexer cluster3.
B. LDAP control is a feature that allows Splunk to integrate with an external LDAP directory service for user authentication and role mapping. LDAP control does not affect distributed search, although it can be used to manage user access to data and searches.
D. Search head clustering is a feature that distributes the search workload across a group of search heads that share resources, configurations, and jobs. Search head clustering does not affect distributed search, although the search heads in a cluster can search across the same set of indexers.

QUESTION 11
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

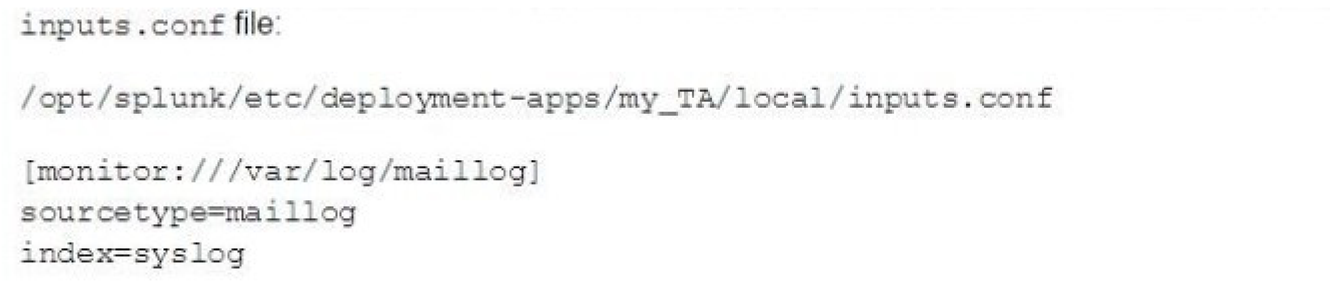
Correct Answer: D
Explanation

QUESTION 12
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:

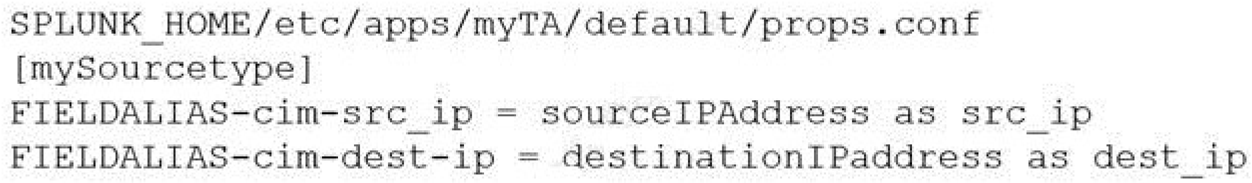
```
/opt/splunk/etc/deployment-apps/my_TA/local/inputs.conf

[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

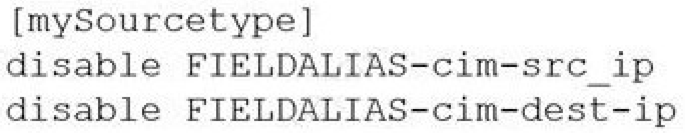
Correct Answer: B
Explanation

QUESTION 13
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?



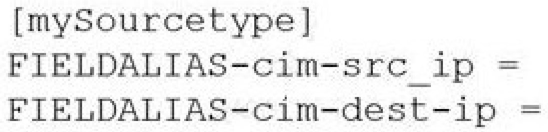
```
SPLUNK_HOME/etc/apps/myTA/default/props.conf
[mySourcetype]
FIELDALIAS-cim-src_ip = sourceIPAddress as src_ip
FIELDALIAS-cim-dest-ip = destinationIPaddress as dest_ip
```

A.



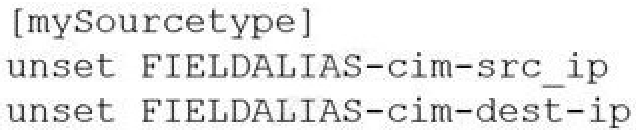
```
[mySourcetype]
disable FIELDALIAS-cim-src_ip
disable FIELDALIAS-cim-dest-ip
```

B.



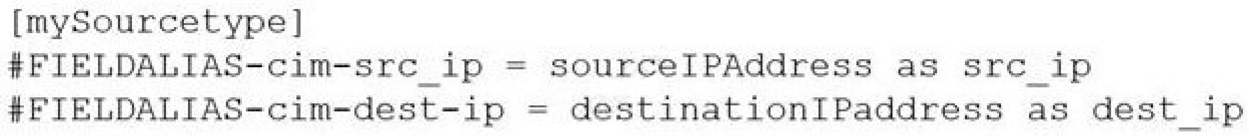
```
[mySourcetype]
FIELDALIAS-cim-src_ip =
FIELDALIAS-cim-dest-ip =
```

C.



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

D.



```
[mySourcetype]
#FIELDALIAS-cim-src_ip = sourceIPAddress as src_ip
#FIELDALIAS-cim-dest-ip = destinationIPaddress as dest_ip
```

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

Correct Answer: B
Explanation

Explanation/Reference:
https://docs.splunk.com/Documentation/Splunk/latest/Admin/Howtoeditaconfigurationfile#Clear%20a%20setting

QUESTION 14
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>

Correct Answer: C
Explanation

Explanation/Reference:
Reference:https://community.splunk.com/t5/Getting-Data-In/How-can-I-trigger-the-re- indexing-of-a-single-file/m-p/108568

The fishbucket is a directory that stores information about the files that have been monitored and indexed by Splunk. The fishbucket helps Splunk avoid indexing duplicate data by keeping track of file signatures and offsets. To reset the fishbucket for one source, the command splunk cmd btprobe can be used with the -reset option and the name of the source file. Therefore, option C is the correct answer. References: Splunk Enterprise Certified Admin | Splunk, [Use btprobe to troubleshoot file monitoring - Splunk Documentation]

QUESTION 15
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.

Correct Answer: A
Explanation

Explanation/Reference:
According to the Splunk documentation1, a heavy forwarder is a Splunk Enterprise instance that can parse and filter data before forwarding it to an indexer. A heavy forwarder can perform line breaking, which is the process of splitting incoming data into individual events based on a set of rules2. A heavy forwarder can also apply other transformations to the data, such as field extractions, event type matching, or masking sensitive data3.

QUESTION 16
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.

Correct Answer: D
Explanation

Explanation/Reference:
The correct answer is D. No, because the event time is greater than the retention time.
According to the Splunk documentation1, the frozenTimePeriodInSecs setting in indexes.conf determines how long Splunk software retains indexed data before deleting it or archiving it to a remote storage. The default value is 188697600 seconds, which is equivalent to six years. The setting can be overridden on a per-index basis. In this case, the cat_facts index has a frozenTimePeriodInSecs setting of 2630000 seconds, which is equivalent to about 30 days. This means that any event that is older than 30 days from the current time will be removed from the index and will not be searchable. The event timestamp was 3739283 seconds ago, which is equivalent to about 43 days. This means that the event is older than the retention time of the cat_facts index and will not be searchable.
The other settings in the stanza, such as maxHotSpanSecs and maxTota1DataSizeMB, do not affect the retention time of the events. They only affect the size and duration of the buckets that store the events.
References:1:Set a retirement and archiving policy - Splunk Documentation

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: AB
Explanation

Explanation/Reference:
According to the Splunk system admin course PDF, When adding native users, Username and Password ARE REQUIRED

QUESTION 18
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: ABD
Explanation

Explanation/Reference:
https://docs.splunk.com/Documentation/Forwarder/8.2.1/Forwarder/HowtoforwarddatatoSpl unkEnterprise "You can collect data on the universal forwarder using several methods. Define inputs on the universal forwarder with the CLI. You can use the CLI to define inputs on the universal forwarder. After you define the inputs, the universal forwarder collects data based on those definitions as long as it has access to the data that you want to monitor. Define inputs on the universal forwarder with configuration files. If the input you want to configure does not have a CLI argument for it, you can configure inputs with configuration files. Create an inputs.conf file in the directory, $SPLUNK_HOME/etc/system/local

QUESTION 19
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.

Correct Answer: AC
Explanation

Explanation/Reference:
The possible causes of the load balancing issue on the Universal Forwarder are A and C. The receiving port and the DNS record are both factors that affect the ability of the Universal Forwarder to distribute data across multiple receivers. If the receiving port is not properly set up to listen on the right port, or if the DNS record used is not set up with a valid list of IP addresses, the Universal Forwarder might fail to connect to some or all of the receivers, resulting in poor load balancing.

QUESTION 20
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. durableQueueSize
C. persistentOueueSize
D. queueSize

Correct Answer: C
Explanation

Explanation/Reference:
Reference:https://docs.splunk.com/Documentation/SplunkCloud/8.2.2111/Data/Usepersistentqueues

QUESTION 21
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

Correct Answer: A
Explanation

QUESTION 22
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.

Correct Answer: AD
Explanation

Explanation/Reference:
https://docs.splunk.com/Documentation/Splunk/8.2.2/Data/Howdoyouwanttoadddata The fastest way to add data to your Splunk Cloud instance or Splunk Enterprise deployment is to use Splunk Web. After you access the Add Data page, choose one of three options for getting data into your Splunk platform deployment with Splunk Web: (1) Upload, (2) Monitor, (3) Forward The Upload option lets you upload a file or archive of files for indexing. When you choose Upload option, Splunk Web opens the upload process page. Monitor. For Splunk Enterprise installations, the Monitor option lets you monitor one or more files, directories, network streams, scripts, Event Logs (on Windows hosts only), performance metrics, or any other type of machine data that the Splunk Enterprise instance has access to.

QUESTION 23
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
Explanation

Explanation/Reference:
"When ingesting event data, the measured data volume is based on the new raw data that is placed into the indexing pipeline. Because the data is measured at the indexing pipeline, data that is filetered and dropped prior to indexing does not count against the license volume qota."
https://docs.splunk.com/Documentation/Splunk/8.0.6/Admin/HowSplunklicensingworks

QUESTION 24
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

Correct Answer: C
Explanation

Explanation/Reference:
The answer to your question is C. services/data/collector. This is the endpoint URI used to collect data in a customer managed Splunk Enterprise environment.According to the Splunk documentation1, "The HTTP Event Collector REST API endpoint is /services/data/collector.You can use this endpoint to send events to HTTP Event Collector on a Splunk Enterprise or Splunk Cloud Platform deployment." You can also use this endpoint to send events to a specific token or index1. For example, you can use thefollowing curl command to send an event with the token 578254cc-05f5-46b5-957b- 910d1400341a and the index main: curl -k https://localhost:8088/services/data/collector -H'Authorization: Splunk 578254cc- 05f5-46b5-957b-910d1400341a'-d'{"index":"main","event":"Hello, world!"}'

QUESTION 25
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]

Correct Answer: B
Explanation

Explanation/Reference:
[monitor::/opt/log/crashlog/Jan27crash.txt]. This stanza means that Splunk is monitoring a single local file named Jan27crash.txt in the /opt/log/crashlog/ directory1. The monitor input type is used to monitor files and directories for changes and index any new data that is added2.

QUESTION 26
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.

Correct Answer: D
Explanation

Explanation/Reference:
The correct answer is D. The timezone of the forwarder will be added to the event as part of indexing.
According to the Splunk documentation1, Splunk software determines the time zone to assign to a timestamp using the following logic in order of precedence:
Use the time zone specified in raw event data (for example, PST, -0800), if present.
Use the TZ attribute set in props.conf, if the event matches the host, source, or source type that the stanza specifies.
If the forwarder and the receiving indexer are version 6.0 or higher, use the time zone that the forwarder provides.

Use the time zone of the host that indexes the event. In this case, the event does not have a time zone specified in the raw data, nor does it have a TZ attribute set in props.conf. Therefore, the next rule applies, which is to use the time zone that the forwarder provides.A universal forwarder is a lightweight agent that can forward data to a Splunk deployment, and it knows its system time zone and sends that information along with the events to the indexer2.The indexer then converts the event time to UTC and stores it in the _time field1.
The other options are incorrect because:
A. Universal Coordinated Time (UTC) is not the time zone that Splunk adds to the event as part of indexing, but rather the time zone that Splunk uses to store the event time in the _time field.Splunk software converts the event time to UTC based on the time zone that it determines from the rules above1.
B.The timezone of the search head is not relevant for indexing, as the search head is a Splunk component that handles search requests and distributes them to indexers, but it does not process incoming data3.The search head uses the user's timezone setting to determine the time range in UTC that should be searched and to display the timestamp of the results in the user's timezone2. C. The timezone of the indexer that indexed the event is only used as a last resort, if none of the other rules apply.In this case, the forwarder provides the time zone information, so the indexer does not use its own time zone1.

QUESTION 27
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

Correct Answer: A
Explanation

Explanation/Reference:
https://docs.splunk.com/Documentation/Splunk/7.3.1/Admin/Configurationfiledirectories Section titled, Configuration file directories, states "A detailed list of settings for each configuration file is provided in the .spec file names for that configuration file. You can find the latest version of the .spec and .example files in the $SPLUNK_HOME/etc system/README folder of your Splunk Enterprise installation..."

QUESTION 28
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

Correct Answer: D
Explanation

QUESTION 29
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

Correct Answer: D
Explanation

Explanation/Reference:
Adding further clarity and quoting same Splunk reference URL from @giubal"

"To keep configuration settings consistent across peer nodes, configuration files are managed from the cluster master, which pushes the files to the slave-app directories on the peer nodes. Files in the slave-app directories have the highest precedence in a cluster peer's configuration. Here is the expanded precedence order for cluster peers:
1.Slave-app local directories -- highest priority
2. System local directory
3. App local directories
4. Slave-app default directories
5. App default directories
6. System default directory --lowest priority

QUESTION 30
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.

Correct Answer: D
Explanation

Explanation/Reference:
The correct answer is 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. According to the Splunk documentation1, to mask sensitive data from raw events, you need to use the SEDCMD attribute in the props.conf file and the REGEX attribute in the transforms.conf file. The SEDCMD attribute applies a sed expression to the raw data before indexing, while the REGEX attribute defines a regular expression to match the data to be masked.You need to place these files on the Splunk instance that parses the data, which isusually the indexer or the heavy forwarder2. The universal forwarder does not parse the data, so it does not need these files. For source A, the data is routed through a heavy forwarder, which can parse the data before sending it to the indexer. Therefore, you need to place both props.conf and transforms.conf on the heavy forwarder for source A, so that the masking takes place before indexing. For source B, the data is routed directly to the indexer, which parses and indexes the data. Therefore, you need to place both props.conf and transforms.conf on the indexer for source B, so that the masking takes place before indexing.
References:1:Redact data from events - Splunk Documentation2:Where do I configure my Splunk settings? - Splunk Documentation

QUESTION 31
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

Correct Answer: D
Explanation

Explanation/Reference:
When using a directory monitor input, specific source types can be selectively overridden using the props.conf file. According to the Splunk documentation, "You can specify a source type for data based on

its input and source. Specify source type for an input. You can assign the source type for data coming from a specific input, such as /var/log/. If you use Splunk Cloud Platform, use Splunk Web to define source types. If you use Splunk Enterprise, define source types in Splunk Web or by editing the inputs.conf configuration file." However, this method is not very granular and assigns the same source type to all data from an input. To override the source type on a per-event basis, you need to use the props.conf file and the transforms.conf file. The props.conf file contains settings that determine how the Splunk platform processes incoming data, such as how to segment events, extract fields, and assign source types. The transforms.conf file contains settings that modify or filter event dataduring indexing or search time. You can use these files to create rules that match specific patterns in the event data and assign different source types accordingly. For example, you can create a rule that assigns a source type of apache_error to any event that contains the word "error" in the first line.

QUESTION 32
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

Correct Answer: D
Explanation

Explanation/Reference:
The deployer is a Splunk Enterprise instance that you use to distribute apps and certain other configuration updates to search head cluster members. The set of updates that the deployer distributes is called the configuration bundle.

QUESTION 33
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: B
Explanation

Explanation/Reference:
https://docs.splunk.com/Documentation/Splunk/latest/Data/Monitornetworkports

QUESTION 34
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
Explanation

Explanation/Reference:
A Splunk platform instance that responses to search requests from a search head. The term "Search peer" is usually synonymous with the indexer role in a distributed search topology..."

QUESTION 35
When using license pools, volume allocations apply to which Splunk components?

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

Correct Answer: A
Explanation

Explanation/Reference:
When using license pools, volume allocations apply to indexers. A license pool is a group of indexers that share a certain amount of daily indexing volume. The license pool specifies how much data each indexer can index per day, as well as which indexes are available for each indexer. Therefore, option A is the correct answer. References: Splunk Enterprise Certified Admin | Splunk, [Set up and manage license pools - Splunk Documentation]

QUESTION 36
Which forwarder is recommended by Splunk to use in a production environment?

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

Correct Answer: D
Explanation

Explanation/Reference:
Reference:https://community.splunk.com/t5/Getting-Data-In/Splunk-forwarder/m-p/18009

The forwarder that is recommended by Splunk to use in a production environment is the universal forwarder. The universal forwarder is a lightweight Splunk agent that forwards data to indexers or other forwarders. The universal forwarder has a small footprint and consumes minimal system resources. It also supports secure and reliable data forwarding with encryption and acknowledgement features. Therefore, option D is the correct answer. References: Splunk Enterprise Certified Admin | Splunk, [About forwarding and receiving data - Splunk Documentation]

QUESTION 37
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

Correct Answer: D
Explanation

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

QUESTION 38
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

Correct Answer: ABC
Explanation

Explanation/Reference:
https://docs.splunk.com/Documentation/Splunk/8.2.2/Data/Configureyourinputs Add your data to Splunk Enterprise. With Splunk Enterprise, you can add data using Splunk Web or Splunk Apps. In addition to these methods, you also can use the following methods. -The Splunk Command Line Interface (CLI) -The inputs.conf configuration file. When you specify your inputs with Splunk Web or the CLI, the details are saved in a configuartion file on Splunk Enterprise indexer and heavy forwarder instances.

QUESTION 39
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.

Correct Answer: D
Explanation

Explanation/Reference:
This is because the input type is UDP, which is an unreliable protocol that does not guarantee delivery, order, or integrity of the data packets. UDP does not have any mechanism to resend or acknowledge the data packets, so if Splunk is restarted, any data that was in transit or in the buffer may be dropped and not indexed.

QUESTION 40
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

Correct Answer: A
Explanation

Explanation/Reference:
The deployment server is a Splunk component that distributes apps and other configurations to deployment clients, which are Splunk instances that receive updates from the deployment server. The deployment server can push apps to single, non-clustered Splunk instances, as well as universal forwarders, which are lightweight Splunk agents that forward data to indexers. Therefore, option A is the correct answer. References: Splunk Enterprise Certified Admin | Splunk, [About deployment server and forwarder management
- Splunk Documentation]

QUESTION 41
Which Splunk forwarder has a built-in license?

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

Correct Answer: C
Explanation

Explanation/Reference:
Reference:https://community.splunk.com/t5/Getting-Data-In/Do-we-need-a-license-for-Heavy-forwarder/m-p/210451

QUESTION 42
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.

Correct Answer: A
Explanation

Explanation/Reference:
https://docs.splunk.com/Documentation/Splunk/8.0.5/Data/Usingforwardingagents Scroll down to the section Titled, How to configure forwarder inputs, and subsection Here are the main ways that you can configure data inputs on a forwarder Install the app or add- on that contains the inputs you wants

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

QUESTION 43
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

Correct Answer: C
Explanation

Explanation/Reference:
The correct answer is C. MonitorNoHandle. MonitorNoHandle is a type of input stanza that allows a Splunk forwarder to read files on Windows systems as Windows writes to them.It does this by using a kernel-mode filter driver to capture raw data as it gets written to the file1.This input stanza is useful for files that get locked open for writing, such as the Windows DNS server log file2.
The other options are incorrect because:
A. Tail Reader is not a valid input stanza in Splunk.It is a component of the Tailing Processor, which is responsible for monitoring files and directories for new data3. B. Upload is a type of input stanza that allows Splunk to index a single file from a local or network file system.It is not suitable for files that are constantly being updated, as it only indexes the file once and does not monitor it for changes4. D. Monitor is a type of input stanza that allows Splunk to monitor files and directories for new data. However, it may not work for files that Windows prevents Splunk from reading while they are open.In such cases, MonitorNoHandle is a better option2.

A Splunk forwarder is a lightweight agent that can forward data to a Splunk deployment. There are two types of forwarders: universal and heavy.A universal forwarder can only forward data, while a heavy forwarder can also perform parsing, filtering, routing, and aggregation on the data before forwarding it5. An

input stanza is a section in the inputs.conf configuration file that defines the settings for a specific type of input, such as files, directories, network ports, scripts, or Windows event logs. An input stanza starts with a square bracket, followed by the input type and the input path or name. For example, [monitor:///var/log] is an input stanza for monitoring the /var/log directory.
References:
1: Monitor files and directories - Splunk Documentation
2: How to configure props.conf for proper line breaking ... - Splunk Community
3: How Splunk Enterprise monitors files and directories - Splunk Documentation
4: Upload a file - Splunk Documentation
5: Use forwarders to get data into Splunk Enterprise - Splunk Documentation [6]: inputs.conf - Splunk Documentation

QUESTION 44
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.

Correct Answer: D
Explanation

Explanation/Reference:
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 45
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
Explanation

QUESTION 46
In which phase do indexed extractions in props.conf occur?

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

Correct Answer: B
Explanation

Explanation/Reference:
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

QUESTION 47
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

Correct Answer: C
Explanation

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

QUESTION 48
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

Correct Answer: B
Explanation

QUESTION 49
What is the valid option for a [monitor] stanza in inputs.conf?

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

Correct Answer: D
Explanation

Explanation/Reference:
Setting: ignoreOlderThan = <time_window> Description: "Causes the input to stop checking files for updates if the file modification time has passed the <time_window> threshold." Default: 0 (disabled)

QUESTION 50
Which Splunk configuration file is used to enable data integrity checking?

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

Correct Answer: C
Explanation

QUESTION 51
Which setting in indexes. conf allows data retention to be controlled by time?

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

Correct Answer: D
Explanation

Explanation/Reference:
https://docs.splunk.com/Documentation/Splunk/latest/Indexer/Setaretirementandarchivingpolicy

QUESTION 52
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

Correct Answer: C
Explanation

Explanation/Reference:
The correct answer is C. On Deployment Server, $SPLUNK_HOME/etc/deployment-apps. A deployment server is a Splunk Enterprise instance that acts as a centralized configuration manager for any number of other instances, called "deployment clients".A deployment client can be a universal forwarder, a non-clustered indexer, or a search head1.
A deployment app is a directory that contains any content that you want to download to a set of deployment clients.The content can include a Splunk Enterprise app, a set of Splunk Enterprise configurations, or other content, such as scripts, images, and supporting files2. You create a deployment app by creating a directory for it on the deployment server. The default location is $SPLUNK_HOME/etc/deployment-apps, but this is configurable through the repositoryLocation attribute in serverclass.conf. Underneath this location, each app must have its own subdirectory.The name of the subdirectory serves as the app name in the forwarder management interface2.
The other options are incorrect because:
A. On Universal Forwarder, $SPLUNK_HOME/etc/apps. This is the location where the deployment app resides after it is downloaded from the deployment server to the universal forwarder.It is not the location of

the app before it is deployed2. B. On Deployment Server, $SPLUNK_HOME/etc/apps. This is the location where the apps that are specific to the deployment server itself reside.It is not the location where the deployment apps for the clients are stored2. D. On Universal Forwarder, $SPLUNK_HOME/etc/deployment-apps. This is not a valid location for any app on a universal forwarder.The universal forwarder does not act as a deployment server and does not store deployment apps3.

QUESTION 53
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.

Correct Answer: D
Explanation

Explanation/Reference:
The Data Preview feature should be used when validating the parsing of data. The Data Preview feature allows you to preview how Splunk software will index your data before you commit the data to an index.You can use the Data Preview feature to check the following aspects of data parsing1:
Timestamp recognition: You can verify that Splunk software correctly identifies the timestamps of your events and assigns them to the _time field. Event breaking: You can verify that Splunk software correctly breaks your data stream into individual events based on the line breaker and should linemerge settings. Source type assignment: You can verify that Splunk software correctly assigns a source type to your data based on the props.conf file settings. You can also manually override the source type if needed. Field extraction: You can verify that Splunk software correctly extracts fields from your events based on the transforms.conf file settings. You can also use the Interactive Field Extractor (IFX) to create custom field extractions. The Data Preview feature is available in Splunk Web under Settings > Data inputs > Data preview.You can access the Data Preview feature when you add a new input or edit an existing input1.
The other options are incorrect because:
A. When extracting fields for ingested data. The Data Preview feature can be used to verify the field extraction for data that has not been ingested yet, but not for data that has already been indexed.To extract fields from ingested data, you can use the IFX or the rex command in the Search app2.
B. When previewing the data before searching. The Data Preview feature does not allow you to search the data, but only to view how it will be indexed. To preview thedata before searching, you can use the Search app and specify a time range or a sample ratio.
C. When reviewing data on the source host. The Data Preview feature does not access the data on the source host, but only the data that has been uploaded or monitored by Splunk software. To review data on the source host, you can use the Splunk Universal Forwarder or the Splunk Add-on for Unix and Linux.

QUESTION 54
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

Correct Answer: D
Explanation

Explanation/Reference:
--reset Reset the fishbucket for the given key or file in the btree. Resetting the checkpoint for an active monitor input reindexes data, resulting in increased license use.

QUESTION 55
The priority of layered Splunk configuration files depends on the file's:

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

Correct Answer: C
Explanation

Explanation/Reference:
https://docs.splunk.com/Documentation/Splunk/7.3.0/Admin/Wheretofindtheconfigurationfil es
"To determine the order of directories for evaluating configuration file precendence, Splunk software considers each file's context. Configuration files operate in either a global context or in the context of the current app and user"

QUESTION 56
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

Correct Answer: A
Explanation

Explanation/Reference:
A Heavy Forwarder is a Splunk instance that can parse and filter data before forwarding it to another Splunk instance, such as an indexer1. A Heavy Forwarder can also perform index-time field extractions using the TRANSFORMS setting2. The TRANSFORMS setting is used to configure data transformations in the transforms.conf file3. The transforms.conf file contains settings and values that you canuse to configure host and source type overrides, anonymize sensitive data, route events to different indexes, create index-time and search-time field extractions, and set up lookup tables3.
The TRANSFORMS setting can be deployed to the Heavy Forwarder where the syslog files are being monitored, so that the logs can be rerouted based on the event message before they are forwarded to the indexer2. This can improve the performance and efficiency of data processing and indexing2.

QUESTION 57
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

Correct Answer: C
Explanation

Explanation/Reference:
Reference:https://docs.splunk.com/Documentation/SplunkCloud/8.2.2105/Security/
SetupuserauthenticationwithLDAP

Splunk platform attempts native authentication first. If authentication fails outside of a local account that doesn't exist, there is no attempt to use LDAP to log in. This is adapted from precedence of Splunk authentication schema.

QUESTION 58
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

Correct Answer: C
Explanation

Explanation/Reference:
https://docs.splunk.com/Documentation/Splunk/8.1.1/DistSearch/Forwardsearchheaddata Per the provided Splunk reference URL by @hwangho, scroll to section Forward search head data, subsection titled, 2. Configure the search head as a forwarder. "Create an outputs.conf file on the search head that configures the search head for load-balanced forwarding across the set of search peers (indexers)."

Reference: https://community.splunk.com/t5/Getting-Data-In/How-to-configure-search-head-to-forwardinternal-data-to-the/td-p/111658

QUESTION 59
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

Correct Answer: C
Explanation

Explanation/Reference:
The CLI command "Splunk add forward-server indexer:<receiving-port>" is used to define the indexer and the listening port on forwards. The command creates this kind of entry "[tcpout-server://<ip address>:<port>]" in the outputs.conf file.
https://docs.splunk.com/Documentation/Forwarder/8.2.2/Forwarder/Configureforwardingwit houtputs.conf

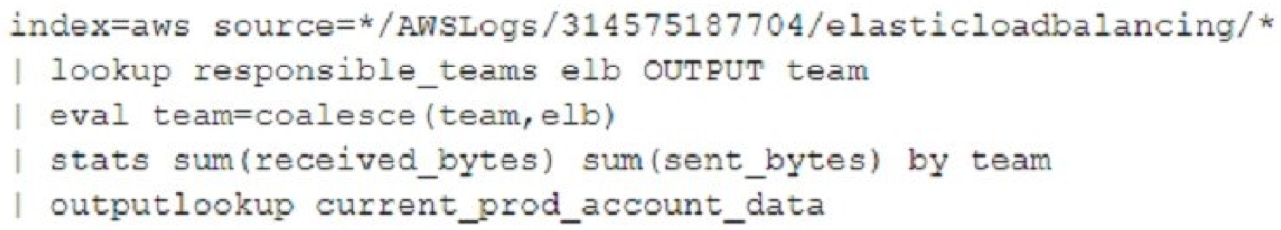
Reference:
https://docs.splunk.com/Documentation/Forwarder/8.0.5/Forwarder/Enableareceiver

QUESTION 60
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
Explanation

QUESTION 61
Running this search in a distributed environment:



```
index=aws source=*/AWSLogs/314575187704/elasticloadbalancing/*
 | lookup responsible_teams elb OUTPUT team
 | eval team=coalesce(team,elb)
 | stats sum(received_bytes) sum(sent_bytes) by team
 | outputlookup current_prod_account_data
```

On what Splunk component does the eval command get executed?

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

Correct Answer: C
Explanation

Explanation/Reference:
The eval command is a distributable streaming command, which means that it can run on the search peers in a distributed environment1. The search peers are the indexers that store the data and perform the initial steps of the search processing2. The eval command calculates an expression and puts the resulting value into a search results field1. In your search, you are using the eval command to create a new field called "responsible_team" based on the values in the "account" field.

QUESTION 62
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: C
Explanation

Explanation/Reference:
https://docs.splunk.com/Documentation/Splunk/7.3.1/DistSearch/Howuserscancontroldistributedsearches
"From the user standpoint, specifying and running a distributed search is essentially the same as running any other search. Behind the scenes, the search head distributes the query to its search peers, and consolidates the results when presenting them to the user."

QUESTION 63
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: ABC
Explanation

Explanation/Reference:
https://docs.splunk.com/Documentation/Splunk/latest/Admin/Wheretofindtheconfigurationfiles
To determine the order of directories for evaluating configuration file precedence, Splunk software

considers each file's context. Configuration files operate in either a global context or inthe context of the current app and user: Global. Activities like indexing take place in a global context. They are independent of any app or user. For example, configuration files that determine monitoring or indexing behavior occur outside of the app and user context and are global in nature. App/ user. Some activities, like searching, take place in an app or user context. The app and user context is vital to search-time processing, where certain knowledge objects or actions might be valid only for specific users in specific apps.

QUESTION 64
Which data pipeline phase is the last opportunity for defining event boundaries?

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

Correct Answer: C
Explanation

Explanation/Reference:
Referencehttps://docs.splunk.com/Documentation/Splunk/8.2.3/Admin/Configurationparametersandthedatapipeline

The parsing phase is the process of extracting fields and values from raw data. The parsing phase respects LINE_BREAKER, SHOULD_LINEMERGE, BREAK_ONLY_BEFORE_DATE, and all other line merging settings in props.conf. These settings determine how Splunk breaks the data into events based on certain criteria, such as timestamps or regular expressions. The event boundaries are defined by the props.conf file, which can be modified by the administrator. Therefore, the parsing phase is the last opportunity for defining event boundaries.

QUESTION 65
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.

Correct Answer: B
Explanation

Explanation/Reference:
Reference:https://docs.splunk.com/Documentation/Splunk/8.2.1/Admin/StartSplunk

https://docs.splunk.com/Documentation/Splunk/8.2.2/Updating/Deploymentserverarchitecture

"A deployment client is a Splunk instance remotely configured by a deployment server".

QUESTION 66
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

Correct Answer: D
Explanation

Explanation/Reference:
The coldPath parameter defines the path for the cold buckets, which are the oldest and least frequently accessed data in an index. By setting the coldPath to point to the NAS mount point, the Splunk administrator can achieve the retention strategy of having older data on slower NAS storage.

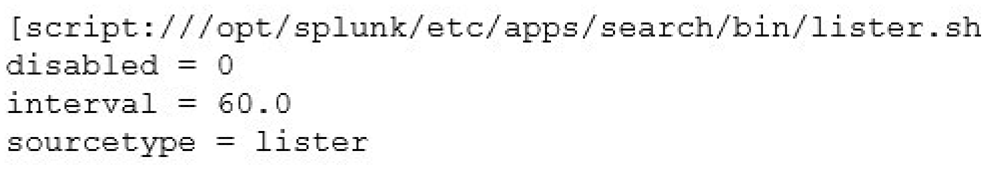
QUESTION 67
All search-time field extractions should be specified on which Splunk component?

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

Correct Answer: D
Explanation

Explanation/Reference:
Search-time field extractions are the process of extracting fields from events after they are indexed. Search-time field extractions are specified on the search head, which is the Splunk component that handles searching and reporting. Search- time field extractions are configured in props.conf and transforms.conf files, which are located in the etc/system/local directory on the search head. Therefore, option D is the correct answer. References: Splunk Enterprise Certified Admin | Splunk, [About fields - Splunk Documentation]

QUESTION 68
Consider the following stanza ininputs.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

Correct Answer: A
Explanation

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

-Scroll down to source = <string>
*Default: the input file path

QUESTION 69
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

Correct Answer: D
Explanation

Explanation/Reference:
https://docs.splunk.com/Documentation/Splunk/8.2.2/Data/Anonymizedata Scrolling down to the section titled "Define the sed script in props.conf shows the correct syntax of an example which validates that the number/character /1 immediately preceded the /g

QUESTION 70
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

Correct Answer: A
Explanation

Explanation/Reference:
Per the provided reference URLhttps://docs.splunk.com/Documentation/Splunk/7.3.1/Admin/User-seedconf "To set the default username and password, place user-seed.conf in $SPLUNK_HOME/etc/system/local. You must restart Splunk to enable configurations. If the $SPLUNK_HOME/etc/passwd file is present, the settings in this file (user-seed.conf) are not used."

QUESTION 71
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

Correct Answer: A
Explanation

Explanation/Reference:
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 72
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

Correct Answer: A
Explanation

Explanation/Reference:
When Splunk is integrated with LDAP, most of the user attributes are managed by the LDAP server and cannot be changed in the Splunk UI. However, one exception is the default app attribute, which specifies which app a user sees when they log in to Splunk. This attribute can be changed in the Splunk UI by editing the user settings. Therefore, option A is the correct answer. References: Splunk Enterprise Certified Admin | Splunk, [Configure Splunk to use LDAP and map groups - Splunk Documentation]

QUESTION 73
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

Correct Answer: C
Explanation

Explanation/Reference:
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 74
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

Correct Answer: B
Explanation

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

QUESTION 75
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

Correct Answer: D
Explanation

Explanation/Reference:
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 76
Which authentication methods are natively supported within Splunk Enterprise? (select all that apply)

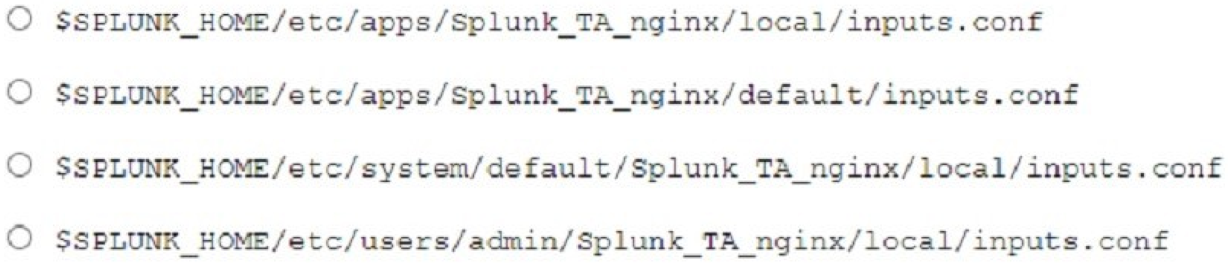
A. LDAP
B. SAML
C. RADIUS
D. Duo Multifactor Authentication

Correct Answer: ABC
Explanation

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

Splunk authentication: Provides Admin, Power and User by default, and you can define your own roles using a list of capabilities. If you have an Enterprise license, Splunk authentication is enabled by default. See Set up user authentication with Splunk's built-in system for more information. LDAP: Splunk Enterprise supports authentication with its internal authentication services or your existing LDAP server. See Set up user authentication with LDAP for more information. Scripted authentication API: Use scripted authentication to integrate Splunk authentication with an external authentication system, such as RADIUS or PAM. See Set up user authentication with external systems for more information. Note: Authentication, including native authentication, LDAP, and scripted authentication, is not available in Splunk Free.

QUESTION 77
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?



○ `$SPLUNK_HOME/etc/apps/Splunk_TA_nginx/local/inputs.conf`

○ `$SPLUNK_HOME/etc/apps/Splunk_TA_nginx/default/inputs.conf`

○ `$SPLUNK_HOME/etc/system/default/Splunk_TA_nginx/local/inputs.conf`

○ `$SPLUNK_HOME/etc/users/admin/Splunk_TA_nginx/local/inputs.conf`

A. Option A
B. Option B

C. Option C
D. Option D

Correct Answer: A
Explanation

Explanation/Reference:
This option corresponds to the file path "$SPLUNK_HOME/etc/apps/splunk_TA_nginx/local/inputs.conf". This is the configuration file that the user needs to edit to ingest the NGINX access logs to ensure it remains unaffected after upgrade.
This is explained in the Splunk documentation, which states:
The local directory is where you place your customized configuration files. The local directory is empty when you install Splunk Enterprise. You create it when you need to override or add to the default settings in a configuration file. The local directory is never overwritten during an upgrade.

QUESTION 78
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.

Correct Answer: C
Explanation

Explanation/Reference:
The app local directories move to second in the priority list. This is explained in the Splunk documentation, which states:
In a clustered environment, the precedence of configuration files changes slightly from that of a standalone deployment. The app local directories move to second in the priority list, after the peer-apps local directory. This means that any configuration files in the app local directories on the individual peers are overridden by configuration files of the same name and type in the peer-apps local directory on the master node.

QUESTION 79
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

Correct Answer: C
Explanation

QUESTION 80
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

Correct Answer: CD
Explanation

Explanation/Reference:

The correct answer is C and D. A heavy forwarder and an indexer are the Splunk components that can break a stream of syslog inputs into individual events. A universal forwarder is a lightweight agent that can forward data to a Splunk deployment, but it does not perform any parsing or indexing on the data. A search head is a Splunk component that handles search requests and distributes them to indexers, but it does not process incoming data. A heavy forwarder is a Splunk component that can perform parsing, filtering, routing, and aggregation on the data before forwarding it to indexers or other destinations.A heavy forwarder can break a stream of syslog inputs into individual events based on the line breaker and should linemerge settings in the inputs.conf file1. An indexer is a Splunk component that stores and indexes data, making it searchable.An indexer can also break a stream of syslog inputs into individual events based on the props.conf file settings, such as TIME_FORMAT, MAX_TIMESTAMP_LOOKAHEAD, and line_breaker2.

A Splunk component is a software process that performs a specific function in a Splunk deployment, such as data collection, data processing, data storage, data search, or data visualization. Syslog is a standard protocol for logging messages from network devices, such as routers, switches, firewalls, or servers. Syslog messages are typically sent over UDP or TCP to a central syslog server or a Splunk instance. Breaking a stream of syslog inputs into individual events means separating the data into discrete records that can be indexed and searched by Splunk. Each event should have a timestamp, a host, a source, and a sourcetype, which are the default fields that Splunk assigns to the data.
References:
1: Configure inputs using Splunk Connect for Syslog - Splunk Documentation
2: inputs.conf - Splunk Documentation
3: How to configure props.conf for proper line breaking ... - Splunk Community
4: Reliable syslog/tcp input ?splunk bundle style | Splunk
5: Configure inputs using Splunk Connect for Syslog - Splunk Documentation
6: About configuration files - Splunk Documentation [7]: Configure your OSSEC server to send data to the Splunk Add-on for OSSEC - Splunk Documentation [8]: Splunk components - Splunk Documentation
[9]: Syslog - Wikipedia
[10]: About default fields - Splunk Documentation

QUESTION 81
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

Correct Answer: A
Explanation

Explanation/Reference:
Reference: https://duo.com/docs/splunk

QUESTION 82
Which of the following Splunk components require a separate installation package?

A. Deployment server
B. License master
C. Universal forwarder
D. Heavy forwarder

Correct Answer: C
Explanation

Explanation/Reference:
Reference:https://github.com/packetiq/SplunkArchitect/blob/master/Install-and-Configure-Splunk-Enterprise-Components.md

The Splunk component that requires a separate installation package is the universal forwarder. The universal forwarder is a lightweight Splunk agent that forwards data to indexers or other forwarders. The universal forwarder has a different installation package than the Splunk Enterprise package, which includes all the other Splunk components. Therefore, option C is the correct answer. References: Splunk Enterprise Certified Admin | Splunk, [About installing Splunk Enterprise with a universal forwarder - Splunk Documentation]

QUESTION 83
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 re-execute 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.

Correct Answer: A
Explanation

Explanation/Reference:
This is explained in the Splunk documentation, which states:
If an indexer goes down during a search, the search head notifies you that the results might be incomplete. The search head does not attempt to re-run the search on another indexer.

QUESTION 84
Which is a valid stanza for a network input?

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

Correct Answer: D
Explanation

QUESTION 85
Which additional component is required for a search head cluster?

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

Correct Answer: A
Explanation

Explanation/Reference:
Reference:https://docs.splunk.com/Documentation/Splunk/8.0.5/DistSearch/SHCdeployme ntoverview

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 86
What event-processing pipelines are used to process data for indexing? (select all that apply)

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

Correct Answer: BD
Explanation

QUESTION 87
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.

Correct Answer: C
Explanation

Explanation/Reference:
"Use serverclass.conf to define server classes" "The most important settings define the set of deployment clients and the set of apps for each server class."

QUESTION 88
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.

Correct Answer: A
Explanation

Explanation/Reference:
https://docs.splunk.com/Documentation/Splunk/8.2.2/Data/AboutHECIDXAck
- Section: About channels and sending data
Sending events to HEC with indexer acknowledgment active is similar to sending them with the setting off. There is one crucial difference: when you have indexer acknowledgment turned on, you must specify a channel when you send events. The concept of a channel was introduced in HEC primarily to prevent a fast client from impeding the performance of a slow client. When you assign one channel per client, because channels are treated equally on Splunk Enterprise, one client can't affect another. You must include a matching channel identifier both when sending data to HEC in an HTTP request and when requesting acknowledgment that events contained in the request have been indexed. If you don't, you will receive the error message, "Data channel is missing." Each request that includes a token for which indexer acknowledgment has been enabled must include a channel identifier, as shown in the following example cURL statement, where <data> represents the event data portion of the request

QUESTION 89
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: A
Explanation

Explanation/Reference:
"The forwarder/indexer relationship can be considered platform agnostic (within the sphere of supported platforms) because they exchange their data handshake (and the data, if you wish) over TCP.

QUESTION 90
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

Correct Answer: A
Explanation

Explanation/Reference:
Reference:https://docs.splunk.com/Documentation/SplunkCloud/latest/Data/Bypassautoma
ticsourcetypeassignment

When using a directory monitor input, specific source types can be selectively overridden using props.conf. The props.conf file contains settings for parsing and indexing data, as well as search-time field extractions. The props.conf file can be used to assign or change source types for specific inputs using the sourcetype attribute. Therefore, option A is the correct answer. References: Splunk Enterprise Certified Admin | Splunk, [Configure directory monitor inputs - Splunk Documentation]

QUESTION 91
Which of the following authentication types requires scripting in Splunk?

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

Correct Answer: D
Explanation

Explanation/Reference:
https://answers.splunk.com/answers/131127/scripted-authentication.html Scripted Authentication: An option for Splunk Enterprise authentication. You can use an authentication system that you have in place (such as PAM or RADIUS) by configuring authentication.conf to use a script instead of using LDAP or Splunk Enterprise default authentication.

QUESTION 92
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.

Correct Answer: A
Explanation

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

QUESTION 93
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

Correct Answer: A
Explanation

Explanation/Reference:
The setting that allows the configuration of Splunk to allow events to span over more than one line is SHOULD_LINEMERGE. This setting determines whether consecutive lines from a single source should be concatenated into a single event. If SHOULD_LINEMERGE is set to true, Splunk will attempt to merge multiple lines into one event based on certain criteria, such as timestamps or regular expressions. Therefore, option A is the correct answer. References: Splunk Enterprise Certified Admin | Splunk, [Configure event line merging - Splunk Documentation]

QUESTION 94
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: AB
Explanation

Explanation/Reference:
https://docs.splunk.com/Documentation/Splunk/8.2.2/Admin/Distdeploylicenses#:~:text=Lic ense%20requirements,do%20not%20index%20external%20data.

"All Splunk Enterprise instances functioning as management components needs access to an Enterprise license. Management components include the deployment server, the indexer cluster manager node, the search head cluster deployer, and the monitoring console."

https://docs.splunk.com/Documentation/Splunk/8.2.2/Updating/Aboutdeploymentserver

"The deployment server is the tool for distributing configurations, apps, and content updates to groups of Splunk Enterprise instances."

QUESTION 95
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

Correct Answer: B

Explanation

Explanation/Reference:
https://docs.splunk.com/Documentation/Splunk/7.3.1/DistSearch/SHCarchitecture Scroll down to section titled, How the cluster handles concurrent search quotas, "Overall search quota. This quota determines the maximum number of historical searches (combined scheduled and ad hoc) that the cluster can run concurrently. This quota is configured with max_Searches_per_cpu and related settings in limits.conf."

QUESTION 96
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.

Correct Answer: AC
Explanation

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

Different retention times: You can set different retention policies for different indexes, depending on how long you want to keep the data. For example, you can have an index for security data that has a longer retention time than an index for performance data that has a shorter retention time.

Restrict user permissions: You can set different access permissions for different indexes, depending on who needs to see the data. For example, you can have an index for sensitive data that is only accessible by certain users or roles, and an index for public data that is accessible by everyone.

QUESTION 97
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
Explanation

Explanation/Reference:
REGEX = <regular expression>
* Enter a regular expression to operate on your data.

FORMAT = <string>
* NOTE: This option is valid for both index-time and search-time field extraction. Index-time field extraction configuration require the FORMAT settings. The FORMAT settings is optional for search-time field extraction configurations.
* This setting specifies the format of the event, including any field names or values you want to add.

DEST_KEY = <key>
* NOTE: This setting is only valid for index-time field extractions.
* Specifies where SPLUNK software stores the expanded FORMAT results in accordance with the REGEX match.

QUESTION 98
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
Explanation

Explanation/Reference:
https://docs.splunk.com/Documentation/Splunk/7.0.3/Forwarding/Routeandfilterdatad#Perform_selective_indexing_and_forwarding
Specifies a comma-separated list of tcpout group names. Use this setting to selectively forward your data to specific indexers by specifying the tcpout groups that the forwarder should use when forwarding the data. Define the tcpout group names in the outputs.conf file in [tcpout:<tcpout_group_name>] stanzas. The groups present in defaultGroup in [tcpout] stanza in the outputs.conf file.

QUESTION 99
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.

Correct Answer: D
Explanation

Explanation/Reference:
https://docs.splunk.com/Documentation/Splunk/8.1.1/Indexer/HowSplunkstoresindexes Once further conditions are met (for example, the index reaches some maximum number of warm buckets), the indexer begins to roll the warm buckets to cold, based on their age. It alwaysselects the oldest warm bucket to roll to cold. Buckets continue to roll to cold as they age in this manner. Cold buckets reside in a different location from hot and warm buckets. You can configure the location so that cold buckets reside on cheaper storage.

Reference: https://community.splunk.com/t5/Deployment-Architecture/Rolling-Hot-Data-to- to-Cold-quicker/tdp/166653

QUESTION 100
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

Correct Answer: C
Explanation

Explanation/Reference:
Indexers, search head, deployment server, license master, universal forwarder. This is the combination of Splunk component instances that are needed to handle the volume of data from collecting log files from 50 Linux servers and 200 Windows servers, following the best practices. The roles and functions of these components are:
Indexers: These are the Splunk instances that index the data and make it searchable. They also perform some data processing, such as timestamp extraction, line breaking, and field extraction. Multiple indexers can be clustered together to provide high availability, data replication, and load balancing. Search head: This is the Splunk instance that coordinates the search across the indexers and merges the results from

them. It also provides the user interface for searching, reporting, and dashboarding. A search head can also be clustered with other search heads to provide high availability, scalability, and load balancing. Deployment server: This is the Splunk instance that manages the configuration and app deployment for the universal forwarders. It allows the administrator to centrally control the inputs.conf, outputs.conf, and other configuration files for the forwarders, as well as distribute apps and updates to them. License master: This is the Splunk instance that manages the licensing for the entire Splunk deployment. It tracks the license usage of all the Splunk instances and enforces the license limits and violations. It also allows the administrator to add, remove, or change licenses.

Universal forwarder: These are the lightweight Splunk instances that collect data from various sources and forward it to the indexers or other forwarders. They do not index or parse the data, but only perform minimal processing, such as compression and encryption. They are installed on the Linux and Windows servers that generate the log files.

QUESTION 101

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: AC

Explanation

QUESTION 102

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_

Correct Answer: ACD

Explanation

Explanation/Reference:

"Where to place the scripts for scripted inputs. The script that you refer to in $SCRIPT can reside in only one of the following places on the host file system:

$SPLUNK_HOME/etc/system/bin

$SPLUNK_HOME/etc/apps/<your_App>/bin

$SPLUNK_HOME/bin/scripts

As a best practice, put your script in the bin/ directory that is nearest to the inputs.conf file that calls your script on the host file system."

QUESTION 103

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

A. Host

B. Server

C. Source

D. Sourcetype

Correct Answer: ACD

Explanation

Explanation/Reference:

https://docs.splunk.com/Documentation/Splunk/8.0.4/Admin/Propsconf#props.conf.spec https://docs.splunk.com/Documentation/Splunk/8.1.1/Admin/Propsconf "* Reuse of the same field-extracting regular expression across multiple sources, source types, or hosts."https://docs.splunk.com/Documentation/Splunk/8.0.4/Admin/Propsconf#props.conf.spec

QUESTION 104
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
Explanation

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

[tcp://<remote server>:<port>]
*Configures the input to listen on a specific TCP network port. *If a <remote server> makes a connection to this instance, the input uses this stanza to configure itself.
*If you do not specify <remote server>, this stanza matches all connections on the specified port.
*Generates events with source set to "tcp:<port>", for example: tcp:514 *If you do not specify a sourcetype, generates events with sourcetype set to "tcp-raw"

QUESTION 105
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

Correct Answer: B
Explanation

Explanation/Reference:
SAML is an open standard for exchanging authentication and authorization data between parties, especially between an identity provider and a service provider1. SAML supports multi-factor authentication by allowing the identity provider to require the user to present two or more factors of evidence to prove their identity2. For example, the user may need to enter a password and a one-time code sent to their phone, or scan their fingerprint and face.

QUESTION 106
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.

Correct Answer: B
Explanation

Explanation/Reference:
"The Splunk platform collects remote Windows data for indexing in one of two ways: From Splunk forwarders, Using Windows Management Instrumentation (WMI). For Splunk Cloud deployments, you must use the Splunk Universal Forwarder on a Windows machines to montior remote Windows data."

QUESTION 107
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: BC
Explanation

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

QUESTION 108
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

Correct Answer: D
Explanation

Explanation/Reference:
Reference:https://docs.splunk.com/Documentation/Splunk/8.2.1/Data/Configuretimestampr ecognition

QUESTION 109
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
Explanation

QUESTION 110
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: B
Explanation

Explanation/Reference:
https://docs.splunk.com/Documentation/Splunk/8.0.6/Security/ManageSplunkuserroleswith LDAP

QUESTION 111
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.

Correct Answer: AC
Explanation

Explanation/Reference:
The correct methods to connect a deployment client to a deployment server are A and C. You can either run the command splunk set deploy-poll <IP_address/hostname>:<management_port> from the command line of the deployment client1 or create and edit a deploymentclient.conf file in $SPLUNK_HOME/etc/ system/local on the deployment client2. Both methods require you to specify the IP address, hostname, and management port of the deployment server that you want the client to connect to.

QUESTION 112
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.

Correct Answer: D
Explanation

Explanation/Reference:
"The search head replicates the knowledge bundle periodically in the background or when initiating a search. " "As part of the distributed search process, the search head replicates and distributes its knowledge objects to its search peers, or indexers. Knowledge objects include saved searches, event types, and other entities used in searching accorss indexes. The search head needs to distribute this material to its search peers so that they can properly execute queries on its behalf."

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

QUESTION 113
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.

Correct Answer: C
Explanation

Explanation/Reference:
The ellipsis wildcard searches recursively through directories and any number of levels of subdirectories to find matches.
If you specify a folder separator (for example, //var/log/.../file), it does not match the first folder level, only subfolders.
* The asterisk wildcard matches anything in that specific folder path segment. Unlike ..., * does not recurse through subfolders.

QUESTION 114
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.

Correct Answer: D
Explanation

Explanation/Reference:
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. This is explained in the Splunk documentation, which states:
To enable automatic load balancing, 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. For example:
[tcpout] server=10.1.1.1:9997,10.1.1.2:9997,10.1.1.3:9997 The forwarder then distributes data across all of the indexers in the list.

QUESTION 115
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

Correct Answer: B
Explanation

Explanation/Reference:
The power role is a default Splunk role that grants users the ability to create saved searches, edit shared objects and alerts, and access advanced search commands. However, the power role does not allow users to create custom roles, which is a privilege reserved for the admin role. Therefore, option B is the correct answer. References: Splunk Enterprise Certified Admin | Splunk, [About configuring role-based user access - Splunk Documentation]

QUESTION 116
What is the correct order of steps in Duo Multifactor Authentication?

A. 1 Request Login
2. Connect to SAML server
3 Duo MFA
4 Create User session
5 Authentication Granted 6. Log into Splunk
B. 1. Request Login 2 Duo MFA
3. Authentication Granted 4 Connect to SAML server
5. Log into Splunk
6. Create User session

C. 1 Request Login
2 Check authentication / group mapping
3 Authentication Granted
4. Duo MFA
5. Create User session
6. Log into Splunk

D. 1 Request Login 2 Duo MFA
3. Check authentication / group mapping
4 Create User session
5. Authentication Granted
6 Log into Splunk

Correct Answer: C
Explanation

Explanation/Reference:
Using the provided DUO/Splunk reference URLhttps://duo.com/docs/splunk

Scroll down to the Network Diagram section and note the following 6 similar steps
1 - SPlunk connection initiated
2 - Primary authentication
3 - Splunk connection established to Duo Security over TCP port 443
4 - Secondary authentication via Duo Security's service
5 - Splunk receives authentication response
6 - Splunk session logged in.

QUESTION 117
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
Explanation

Explanation/Reference:
<https://docs.splunk.com/Documentation/Splunk/8.0.6/Updating/Deploymentserverarchitect ure>
https://docs.splunk.com/Splexicon:Serverclass

QUESTION 118
Which artifact is required in the request header when creating an HTTP event?

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

Correct Answer: B
Explanation

Explanation/Reference:
Reference:https://docs.splunk.com/Documentation/Splunk/8.2.3/Data/FormateventsforHTT PEventCollector

When creating an HTTP event, the request header must include a token that identifies the HTTP Event Collector (HEC) endpoint. The token is a 32-character hexadecimal string that is generated when the HEC endpoint is created. The token is used to authenticate the request and route the event data to the correct index. Therefore, option B is the correct answer. References: Splunk Enterprise Certified Admin | Splunk,

[About HTTP Event Collector - Splunk Documentation]

QUESTION 119
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

Correct Answer: CD
Explanation

Explanation/Reference:
Reference: https://wiki.splunk.com/Deploy:BucketRotationAndRetention

QUESTION 120
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

Correct Answer: C
Explanation

Explanation/Reference:
The correct answer is C. /var/log/host_460352847/bar/file/foo.txt. The monitor stanza in inputs.conf is used to configure Splunk to monitor files and directories for new data.The monitor stanza has the following syntax1:
[monitor://<input path>]
The input path can be a file or a directory, and it can include wildcards (*) and regular expressions. The wildcards match any number of characters, including none, while the regular expressions match patterns of characters.The input path is case-sensitive and must be enclosed in double quotes if it contains spaces1. In this case, the input path is /var/log//bar/.txt, which means Splunk will monitor any file with the .txt extension that is located in a subdirectory named bar under the / var/log directory.The subdirectory bar can be at any level under the /var/log directory, and the * wildcard will match any characters before or after the bar and .txt parts1. Therefore, the file /var/log/host_460352847/bar/file/foo.txt will be matched by the monitor stanza, as it meets the criteria. The other files will not be matched, because:
A. /var/log/host_460352847/temp/bar/file/csv/foo.txt has a .csv extension, not a .txt extension.
B. /var/log/host_460352847/bar/foo.txt is not located in a subdirectory under the bar directory, but directly in the bar directory. D. /var/log/host_460352847/temp/bar/file/foo.txt is located in a subdirectory named file under the bar directory, not directly in the bar directory.

Exam B

QUESTION 1
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

Correct Answer: A
Explanation

Explanation/Reference:
https://www.splunk.com/en_us/blog/tips-and-tricks/what-is-this-fishbucket- thing.html
"Every Splunk instance has a fishbucket index, except the lightest of hand-tuned lightweight forwarders, and if you index a lot of files it can get quite large. As any other index, you can change the retention policy to control the size via indexes.conf"

Reference https://community.splunk.com/t5/Archive/How-to-reindex-data-from-a- forwarder/td-p/93310

QUESTION 2
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: C
Explanation

Explanation/Reference:
https://docs.splunk.com/Documentation/Splunk/8.0.3/Data/Monitornetworkports

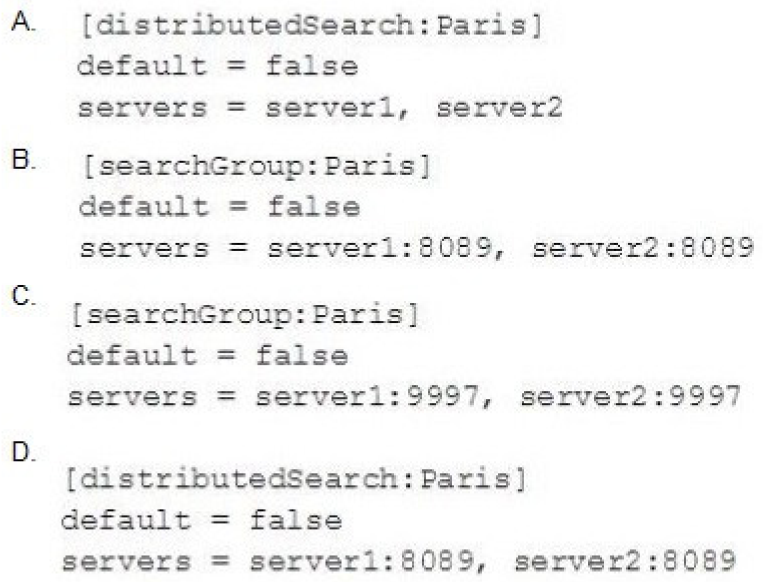
QUESTION 3
In which Splunk configuration is the SEDCMD used?

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

Correct Answer: A
Explanation

Explanation/Reference:
https://docs.splunk.com/Documentation/Splunk/8.0.5/Forwarding/Forwarddatatothird-partysystemsd
"You can specify a SEDCMD configuration in props.conf to address data that contains characters that the third-party server cannot process. "

QUESTION 4
Which of the following is valid distribute 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
```

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

Correct Answer: D
Explanation

QUESTION 5
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

Correct Answer: B
Explanation

Explanation/Reference:
https://docs.splunk.com/Documentation/Splunk/8.1.3/Security/ConfigureLDAPwithSplunkWeb
"You can map either users or groups, but not both. If you are using groups, all users must be members of an appropriate group. Groups inherit capabilities form the highest level role they're a member of." "If your LDAP environment does not have group entries, you can treat each user as its own group."

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

QUESTION 6
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

Explanation

Explanation/Reference:
https://docs.splunk.com/Documentation/Splunk/latest/Data/Whitelistorblacklistspecificincomingdata#Include_or_exclude_specific_incoming_data

QUESTION 7
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

Correct Answer: BC
Explanation

Explanation/Reference:
The indexing pipeline and the parsing pipeline are the two pipelines that are responsible for transforming the raw data into events and preparing them for indexing. The indexing pipeline applies index-time settings, such as timestamp extraction, line breaking, host extraction, and source type recognition. The parsing pipeline applies parsing settings, such as field extraction, event segmentation, and event annotation.

QUESTION 8
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: BD
Explanation

Explanation/Reference:
https://docs.splunk.com/Documentation/Splunk/8.0.1/Forwarding/Aboutforwardingandreceivingdata
https://docs.splunk.com/Documentation/Forwarder/8.1.1/Forwarder/Configureforwardingwithoutputs.conf#:~:text=compressed%3Dtrue%20This%20tells%20the,the%20forwarder%20 sends%20raw%20data.

QUESTION 9
What is the name of the object that stores events inside of an index?

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

Correct Answer: B
Explanation

Explanation/Reference:
A bucket is the object that stores events inside of an index. According to the Splunk documentation, "An index is a collection of directories, also called buckets, that contain index files. Each bucket represents a specific time range." A bucket can be in one of several states, such as hot, warm, cold, frozen, or thawed. Buckets are managed by indexers or clusters of indexers.

QUESTION 10
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
Explanation

Explanation/Reference:
https://docs.splunk.com/Documentation/Splunk/9.0.0/DistSearch/Distributedsearchgroups

QUESTION 11
Which Splunk component does a search head primarily communicate with?

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

Correct Answer: A
Explanation

QUESTION 12
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

Correct Answer: C
Explanation

Explanation/Reference:
A Splunk Enterprise trial license gives you access to all the features of Splunk Enterprise for a limited period of time, usually 60 days1. After the trial period expires, you can either purchase a Splunk Enterprise license or switch to a Free license.
A Splunk Enterprise Free license allows you to index up to 500 MB of data per day, but some features are disabled, such as authentication, distributed search, and alerting. You can switch to a Free license at any time during the trial period or after the trial period expires.
A Splunk Enterprise Forwarder license is used with forwarders, which are Splunk instances that forward data to other Splunk instances. A Forwarder license does not allow indexing or searching of data. You can install a Forwarder license on any Splunk instance that you want to use as a forwarder. A Splunk Enterprise commercial end-user license is a license that you purchase from Splunk based on either data volume or infrastructure. This license gives you access to all the features of Splunk Enterprise within a defined limit of indexed data per day (volume-based license) or vCPU count (infrastructure license). You can purchase and install this license after the trial period expires or at any time during the trial period1.

QUESTION 13
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.

Correct Answer: C

Explanation

Explanation/Reference:
Quoting the following Splunk URL reference https://docs.splunk.com/Documentation/Splunk/8.2.2/DMC/DMCprerequisites "Monitoring Console setup prerequisites. Forward internal logs (both $SPLUNK_HOME/car/log/splunk and$SPLUNK_HOME/var/log/introspection) to indexers from all other components. Without this step, many dashboards will lack data."

QUESTION 14
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

Correct Answer: B
Explanation

Explanation/Reference:
Reference:https://docs.splunk.com/Documentation/Splunk/8.2.1/Admin/MoreaboutSplunkFree

https://docs.splunk.com/Documentation/Splunk/8.2.3/Admin/TypesofSplunklicenses

QUESTION 15
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

Correct Answer: D
Explanation

Explanation/Reference:
You can have a role inherit certain properties from one or more existing rolehttps://docs.splunk.com/Documentation/Splunk/8.0.5/Security/Aboutusersandroles Reference:
https://docs.splunk.com/Documentation/Splunk/8.0.5/Security/Aboutusersandroles

QUESTION 16
What is the default value ofLINE_BREAKER?

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

Correct Answer: B
Explanation

Explanation/Reference:
Reference:https://docs.splunk.com/Documentation/SplunkCloud/8.2.2105/Data/Configuree ventlinebreaking

Line breaking, which uses the LINE_BREAKER setting to split the incoming stream of data into separate lines. By default, the LINE_BREAKER value is any sequence of newlines and carriage returns. In regular expression format, this is represented as the following string: ([\r\n]+). You don't normally need to adjust this setting, but in cases where it's necessary, you must configure it in the props.conf configuration file on the forwarder that sends the data to Splunk Cloud Platform or a Splunk Enterprise indexer. The LINE_BREAKER setting expects a value in regular expression format.

QUESTION 17
Immediately after installation, what will a Universal Forwarder do first?

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

Correct Answer: C
Explanation

Explanation/Reference:
Begin generating internal Splunk logs. Immediately after installation, a Universal Forwarder will start generating internal Splunk logs that contain information about its own operation, such as startup and shutdown events, configuration changes, data ingestion, and forwarding activities. These logs are stored in the $SPLUNK_HOME/var/log/splunk directory on the Universal Forwarder machine.

QUESTION 18
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.

Correct Answer: C
Explanation

Explanation/Reference:
A Splunk deployment server is a system that distributes apps, configurations, and other assets to groups of Splunk Enterprise instances. You can use it to distribute updates to most types of Splunk Enterprise components: forwarders, non- clustered indexers, and search heads.
A Splunk deployment server is available on every full Splunk Enterprise instance. To use it, you must activate it by placing at least one app into %SPLUNK_HOME%\etc\deployment-apps on the host you want to act as deployment server. A Splunk deployment server maintains the list of server classes and uses those server classes to determine what content to distribute to each client. A server class is a group of deployment clients that share one or more defined characteristics. A Splunk deployment client is a Splunk instance remotely configured by a deployment server. Deployment clients can be universal forwarders, heavy forwarders, indexers, or search heads. Each deployment client belongs to one or more server classes.
A Splunk deployment app is a set of content (including configuration files) maintained on the deployment server and deployed as a unit to clients of a server class. A deployment app can be an existing Splunk Enterprise app or one developed solely to group some content for deployment purposes. Therefore, option C is correct, and the other options are incorrect.

QUESTION 19
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.

Correct Answer: D
Explanation

Explanation/Reference:
When there are conflicting settings within two or more configuration files, the setting with the highest precedence is used. The precedence of configuration files is determined by a combination of the file type, the directory location, and the alphabetical order of the file names.

QUESTION 20
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

Correct Answer: A
Explanation

QUESTION 21
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
Explanation

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

"Configure character set encoding. Splunk software attempts to apply UTF-8 encoding to your scources by default. If a source foesn't use UTF-8 encoding or is a non-ASCII file, Splunk software tries to convert data from the source to UTF-8 encoding unless you specify a character set to use by setting the CHARSET key in the props.conf file."

QUESTION 22
TheLINE_BREAKERattribute is configured in which configuration file?

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

Correct Answer: A
Explanation

Explanation/Reference:
Reference:https://docs.splunk.com/Documentation/SplunkCloud/8.2.2105/Data/Configureeventlinebreaking

QUESTION 23
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

Correct Answer: C
Explanation

Explanation/Reference:
Reference:https://docs.splunk.com/Documentation/Forwarder/8.2.1/Forwarder/Configurelo adbalancing

QUESTION 24
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.

Correct Answer: A
Explanation

Explanation/Reference:
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 25
Event processing occurs at which phase of the data pipeline?

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

Correct Answer: C
Explanation

Explanation/Reference:
According to the Splunk documentation1, event processing occurs at the parsing phase of the data pipeline. The parsing phase is where Splunk software processes incoming data into individual events, extracts timestamp information, assigns source types, and performs other tasks to make the data searchable1. The parsing phase can also apply field extractions, event type matching, and other transformations to the events2.

QUESTION 26
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

Correct Answer: AC
Explanation

Explanation/Reference:
https://docs.splunk.com/Documentation/Forwarder/8.0.5/Forwarder/Configuretheuniversalf orwarder
--Key configuration files are: inputs.conf controls how the forwarder collects data. outputs.conf controls how the forwarder sends data to an indexer or other forwarder server.conf for connection and performance tuning deploymentclient.conf for connecting to a deployment server

Reference: https://docs.splunk.com/Documentation/Forwarder/8.0.5/Forwarder/Configuretheuniversalforwarder

QUESTION 27
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>###-##-$2
KEY = _raw

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

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

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

Correct Answer: D
Explanation

Explanation/Reference:
because transforms.conf is the right configuration file to state the regex expression.https://docs.splunk.com/Documentation/Splunk/8.1.0/Admin/Transformsconf

Reference: https://community.splunk.com/t5/Archive/How-to-mask-SSN-into-our-logs- going-into-Splunk/tdp/433035

QUESTION 28
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
Explanation

Explanation/Reference:
https://docs.splunk.com/Documentation/Splunk/8.2.2/Data/UsetheHTTPEventCollector "The HTTP Event Collector (HEC) lets you send data and application events to a Splunk deployment over the HTTP and Secure HTTP (HTTPS) protocols. HEC uses a token- based authentication model. You can generate a token and then configure a logging library or HTTP client with the token to send data to HEC in a specific format. This process eliminates the need for a Splunk forwarder when you send application events."

QUESTION 29
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.

Correct Answer: B
Explanation

Explanation/Reference:
Immediately after installation, a universal forwarder will start generating internal Splunk logs that contain information about its own operation, such as configuration changes, data inputs, and forwarding activities1. These logs are stored in the $SPLUNK_HOME/var/log/splunk directory on the universal forwarder machine1. The universal forwarder will not automatically detect any indexers in its subnet and begin routing data, as it needs to be configured with the IP address and port number of the indexer or the deployment server2. The universal forwarder will not begin reading local files on its server, as it needs to be configured with the data inputs that specify which files or directories to monitor2. The universal forwarder will not send an email to the operator that the installation process has completed, as this is not a default behavior of the universal forwarder and would require additional configuration3.

QUESTION 30
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

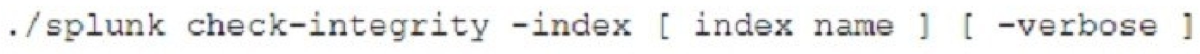
Which of the following is a true statement?

A. Data will continue to flow to hfbank if 145.188.183.184:9097 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 145.183.184:097 is specified by IP.
D. Data will eventually stop flowing everywhere if 145.188.183.184:9097 is unreachable.

Correct Answer: A
Explanation

Explanation/Reference:
The outputs.conf file defines how forwarders send data to receivers1. You can specify some output configurations at installation time (Windows universal forwarders only) or the CLI, but most advanced configuration settings require that you edit outputs.conf1.
The [tcpout:...] stanza specifies a group of forwarding targets that receive data over TCP2. You can define multiple groups with different names and settings2. The server setting lists one or more receiving hosts for the group, separated by commas2. If you specify multiple hosts, the forwarder load balances the data across them2.
Therefore, option A is correct, because the forwarder will send data to both inputsl.mysplunkhfs.corp:9997 and inputs2.mysplunkhfs.corp:9997, even if 145.188.183.184:9097 is unreachable.

QUESTION 31
When would the following command be used?



```
./splunk check-integrity -index [ index name ] [ -verbose ]
```

A. To verify' the integrity of a local index.

B. To verify the integrity of a SmartStore index.

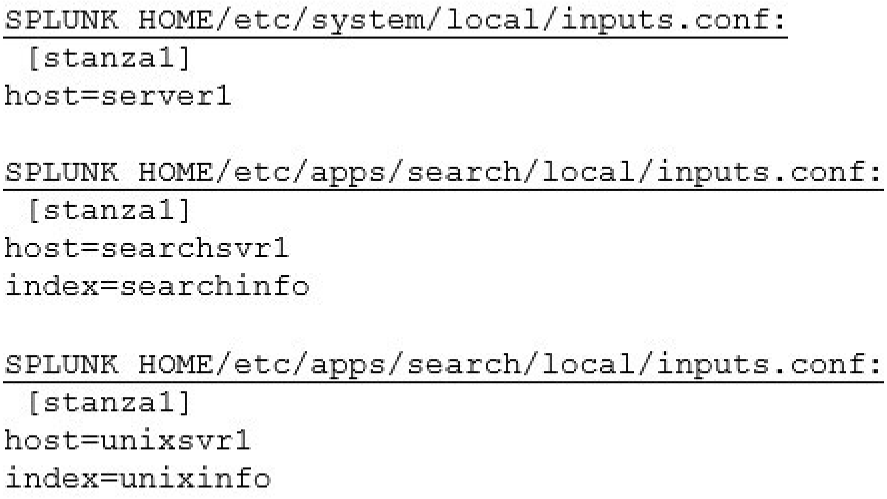
C. To verify the integrity of a SmartStore bucket.

D. To verify the integrity of a local bucket.

Correct Answer: D
Explanation

Explanation/Reference:
To verify the integrity of a local bucket. The command ./splunk check- integrity -bucketPath [bucket path] [-verbose] is used to verify the integrity of a local bucket by comparing the hashes stored in the l1Hashes and l2Hash files with the actual data in the bucket1. This command can help detect any tampering or corruption of the data.

QUESTION 32
What are the values forhostandindexfor[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

Correct Answer: A
Explanation

Explanation/Reference:
- 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 33
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.

Correct Answer: B
Explanation

Explanation/Reference:
https://docs.splunk.com/Documentation/Splunk/8.2.2/DistSearch/Whatisdistributedsearch
Parallel reduce search processing If you struggle with extremely large high-cardinality searches, you might be able to apply parallel reduce processing to them to help them complete faster. You must have a distributed search environment to use parallel reduce search processing.

QUESTION 34
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

Correct Answer: AD
Explanation

Explanation/Reference:
https://docs.splunk.com/Documentation/Splunk/8.1.1/Knowledge/Configureadvancedextractionswithfieldtransforms
use transformations with props.conf and transforms.conf to:
Mask or delete raw data as it is being indexed verride sourcetype or host based upon event values
Route events to specific indexes based on event content ?Prevent unwanted events from being indexed

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

QUESTION 35
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

Correct Answer: A
Explanation

Explanation/Reference:
According to the Splunk documentation1, to manually specify a character set for an input, you need to set the CHARSET key in the props.conf file. You can specify the character set by host, source, or sourcetype, but not by index. https:// docs.splunk.com/Documentation/Splunk/latest/Data/ Configurecharactersetencoding

QUESTION 36
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

Correct Answer: D
Explanation

Explanation/Reference:
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 37
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

Correct Answer: D
Explanation

Explanation/Reference:
After an app is downloaded, it resides under $SPLUNK_HOME/etc/apps on the deployment clients. But it resided in the $SPLUNK_HOME/etc/deployment-apps location in the deployment server.

QUESTION 38
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

Correct Answer: D
Explanation

Explanation/Reference:
Using the Splunk reference URLhttps://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 39
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: ACD
Explanation

Explanation/Reference:

https://docs.splunk.com/Documentation/SplunkCloud/8.2.2106/Admin/ConcurrentLimits "Set limits for concurrent scheduled searches. You must have the edit_search_concurrency_all and edit_search_concurrency_scheduled capabilities to configure these settings."

QUESTION 40
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.

Correct Answer: A
Explanation

Explanation/Reference:
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 41
In case of a conflict between a whitelist and a blacklist input setting, which one is used?

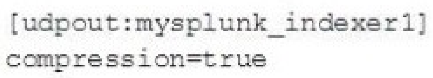
A. Blacklist
B. Whitelist
C. They cancel each other out.
D. Whichever is entered into the configuration first.

Correct Answer: A
Explanation

Explanation/Reference:
https://docs.splunk.com/Documentation/Splunk/8.0.4/Data/Whitelistorblacklistspecificincomi ngdata
"It is not necessary to define both an allow list and a deny list in a configuration stanza. The settings are independent. If you do define both filters and a file matches them both, Splunk Enterprise does not index that file, as the blacklist filter overrides the whitelist filter." Source:https://docs.splunk.com/Documentation/Splunk/8.1.0/Data/Whitelistorblacklistspecif icincomingdata

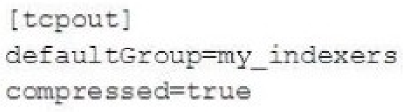
QUESTION 42
Which of the following enables compression for universal forwarders in outputs. conf ?

A.



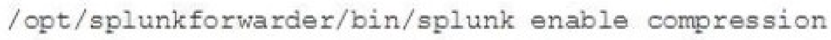
```
[udpout:mysplunk_indexer1]
compression=true
```

B.



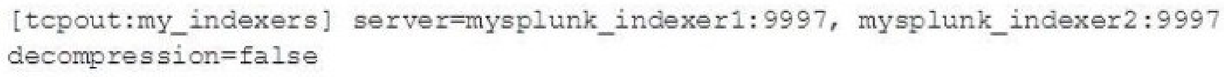
```
[tcpout]
defaultGroup=my_indexers
compressed=true
```

C.



```
/opt/splunkforwarder/bin/splunk enable compression
```

D.



```
[tcpout:my_indexers] server=mysplunk_indexer1:9997, mysplunk_indexer2:9997
decompression=false
```

A. Option A

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

Correct Answer: B
Explanation

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

```
# Compression
#
# This example sends compressed events to the remote indexer. # NOTE: Compression can be enabled TCP or SSL outputs only. # The receiver input port should also have compression enabled.
[tcpout]
server = splunkServer.example.com:4433
compressed = true
```

QUESTION 43
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

Correct Answer: C
Explanation

Explanation/Reference:
"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 44
Which forwarder type can parse data prior to forwarding?

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

Correct Answer: D
Explanation

Explanation/Reference:
https://docs.splunk.com/Documentation/Splunk/latest/Forwarding/Typesofforwarders "A heavy forwarder parses data before forwarding it and can route data based on criteria such as source or type of event."

QUESTION 45
Which of the following indexes come pre-configured with Splunk Enterprise? (select all that apply)

A. _license
B. _Internal
C. _external
D. _thefishbucket

Correct Answer: BD
Explanation

Explanation/Reference:
https://docs.splunk.com/Documentation/Splunk/8.0.5/Indexer/Howindexingworks

QUESTION 46
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

Correct Answer: D
Explanation

Explanation/Reference:
https://docs.splunk.com/Documentation/Splunk/8.0.3/Admin/Distdeploylicenses#Clustered_ deployments_and_licensing_issues

Reference:https://community.splunk.com/t5/Deployment-Architecture/License-usage-in- Indexer-Cluster/m-p/493548

QUESTION 47
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

Correct Answer: D
Explanation

QUESTION 48
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
Explanation

Explanation/Reference:
https://docs.splunk.com/Documentation/Splunk/latest/Data/Configureeventlinebreaking Attribute : SHOULD_LINEMERGE = [true|false]

Description : When set to true, the Splunk platform combines several input lines into a single event, with configuration based on the settings described in the next section.

QUESTION 49
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.

Correct Answer: D
Explanation

Explanation/Reference:
https://docs.splunk.com/Documentation/Splunk/8.2.2/Updating/Aboutdeploymentserver "The deployment server is the tool for distributing configurations, apps, and content updates to groups of Splunk Enterprise instances."

QUESTION 50
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

Correct Answer: A
Explanation

Explanation/Reference:
This is the endpoint URI used to collect data using the HTTP Event Collector (HEC), which is a token-based API that allows you to send data to Splunk Enterprise from any application that can make an HTTP request. The endpoint URI consists of the protocol (http or https), the hostname or IP address of the Splunk server, the port number (default is 8088), and the service name (services/collector). For example: https://mysplunkserver.example.com:8088/services/collector

QUESTION 51
What is the correct example to redact a plain-text password from raw events?

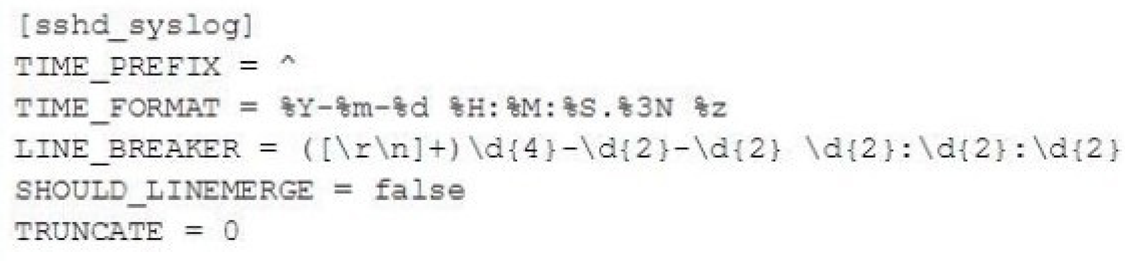
A. in props.conf:
[identity]
REGEX-redact_pw = s/password=([^,|/s]+)/ ####REACTED####/g
B. in props.conf:
[identity]
SEDCMD-redact_pw = s/password=([^,|/s]+)/ ####REACTED####/g
C. in transforms.conf:
[identity]
SEDCMD-redact_pw = s/password=([^,|/s]+)/ ####REACTED####/g
D. in transforms.conf:
[identity]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

Correct Answer: B
Explanation

Explanation/Reference:
The correct answer is B. in props.conf:
[identity]
SEDCMD-redact_pw = s/password=([^,|/s]+)/ ####REACTED####/g According to the Splunk documentation1, to redact sensitive data from raw events, you need to use the SEDCMD attribute in the props.conf file. The SEDCMD attribute applies a sed expression to the raw data before indexing. The sed expression can use the s command to replace a pattern with a substitution string. For example, the following sed expression replaces any occurrence of password= followed by any characters until a comma, whitespace, or slash with ####REACTED####:
s/password=([^,|/s]+)/ ####REACTED####/g
The g flag at the end means that the replacement is applied globally, not just to the first match.
Option A is incorrect because it uses the REGEX attribute instead of the SEDCMD attribute. The REGEX

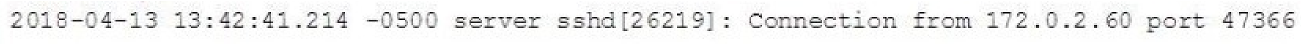
attribute is used to extract fields from events, not to modify them. Option C is incorrect because it uses the transforms.conf file instead of the props.conf file. The transforms.conf file is used to define transformations that can be applied to fields or events, such as lookups, evaluations, or replacements. However, these transformations are applied after indexing, not before. Option D is incorrect because it uses both the wrong attribute and the wrong file. There is no REGEX-redact_pw attribute in the transforms.conf file.
References:1:Redact data from events - Splunk Documentation

QUESTION 52
In this source definition the MAX_TIMESTAMP_LOOKHEAD 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}
SHOULD_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_L0CKAHEAD = 5
B. MAX_TIMESTAMP_LOOKAHEAD - 10
C. MAX_TIMESTAMF_LOOKHEAD = 20
D. MAX TIMESTAMP LOOKAHEAD - 30

Correct Answer: D
Explanation

Explanation/Reference:
https://docs.splunk.com/Documentation/Splunk/6.2.0/Data/Configuretimestamprecognition "Specify how far (how many characters) into an event Splunk software should look for a timestamp." since TIME_PREFIX = ^ and timestamp is from 0- 29 position, so D=30 will pick up the WHOLE timestamp correctly.

QUESTION 53
A new forwarder has been installed with a manually createddeploymentclient.conf.

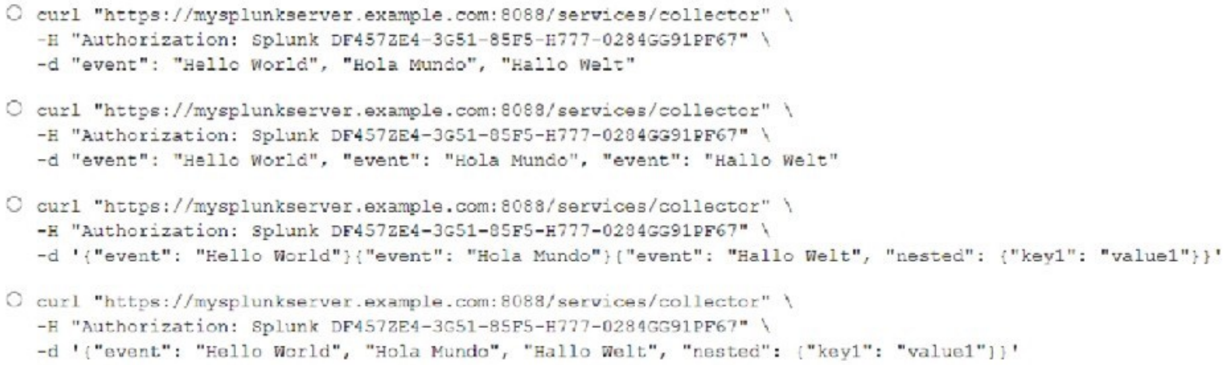
What is the next step to enable the communication between the forwarder and the deployment server?

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.

Correct Answer: C
Explanation

Explanation/Reference:
The next step to enable the communication between the forwarder and the deployment server after installing a new forwarder with a manually created deploymentclient.conf is to restart Splunk on the deployment client. The deploymentclient.conf file contains the settings for the deployment client, which is a Splunk instance that receives updates from the deployment server. The file must include the targetUri attribute, which specifies the hostname and management port of the deployment server. To apply the changes in the deploymentclient.conf file, Splunk must be restarted on the deployment client. Therefore, option C is the correct answer. References: Splunk Enterprise Certified Admin | Splunk, [Configure deployment clients - Splunk Documentation]

QUESTION 54
What is the correct curl to send multiple events through HTTP Event Collector?



```
○ curl "https://mysplunkserver.example.com:8088/services/collector" \
  -H "Authorization: Splunk DF457ZE4-3G51-85F5-H777-0284GG91PF67" \
  -d "event": "Hello World", "Hola Mundo", "Hallo Welt"

○ curl "https://mysplunkserver.example.com:8088/services/collector" \
  -H "Authorization: Splunk DF457ZE4-3G51-85F5-H777-0284GG91PF67" \
  -d "event": "Hello World", "event": "Hola Mundo", "event": "Hallo Welt"

○ curl "https://mysplunkserver.example.com:8088/services/collector" \
  -H "Authorization: Splunk DF457ZE4-3G51-85F5-H777-0284GG91PF67" \
  -d '{"event": "Hello World"}{"event": "Hola Mundo"}{"event": "Hallo Welt", "nested": {"key1": "value1"}}'

○ curl "https://mysplunkserver.example.com:8088/services/collector" \
  -H "Authorization: Splunk DF457ZE4-3G51-85F5-H777-0284GG91PF67" \
  -d '{"event": "Hello World", "Hola Mundo", "Hallo Welt", "nested": {"key1": "value1"}}'
```

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

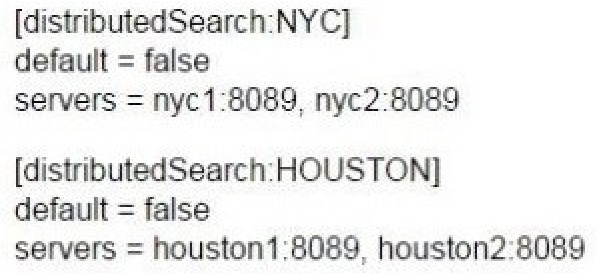
Correct Answer: B
Explanation

Explanation/Reference:
curl "https://mysplunkserver.example.com:8088/services/collector" \ -H "Authorization: Splunk DF4S7ZE4-3GS1-8SFS-E777-0284GG91PF67" \ -d `{"event": "Hello World"}, {"event": "Hola Mundo"}, {"event": "Hallo Welt"}'. This is the correct curl command to send multiple events through HTTP Event Collector (HEC), which is a token-based API that allows you to send data to Splunk Enterprise from any application that can make an HTTP request. The command has the following components:
The URL of the HEC endpoint, which consists of the protocol (https), the hostname or IP address of the Splunk server (mysplunkserver.example.com), the port number (8088), and the service name (services/collector). The header that contains the authorization token, which is a unique identifier that grants access to the HEC endpoint. The token is prefixed with Splunk and enclosed in quotation marks. The token value (DF4S7ZE4-3GS1-8SFS-E777- 0284GG91PF67) is an example and should be replaced with your own token value.
The data payload that contains the events to be sent, which are JSON objects enclosed in curly braces and separated by commas. Each event object has a mandatory field called event, which contains the raw data to be indexed. The event value can be a string, a number, a boolean, an array, or another JSON object. In this case, the event values are strings that say hello in different languages.

QUESTION 55
How would you configure your distsearch conf to allow you to run the search below?

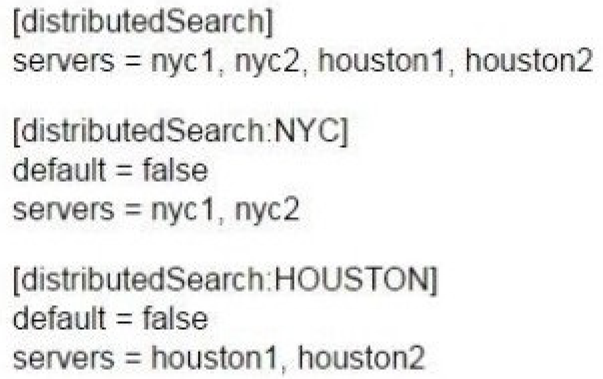
sourcetype=access_combined status=200 action=purchase splunk_setver_group=HOUSTON

A.



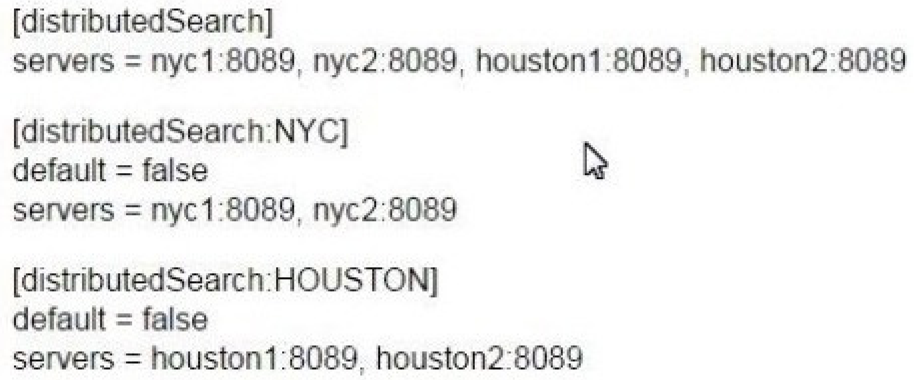
```
[distributedSearch:NYC]
default = false
servers = nyc1:8089, nyc2:8089

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

B.



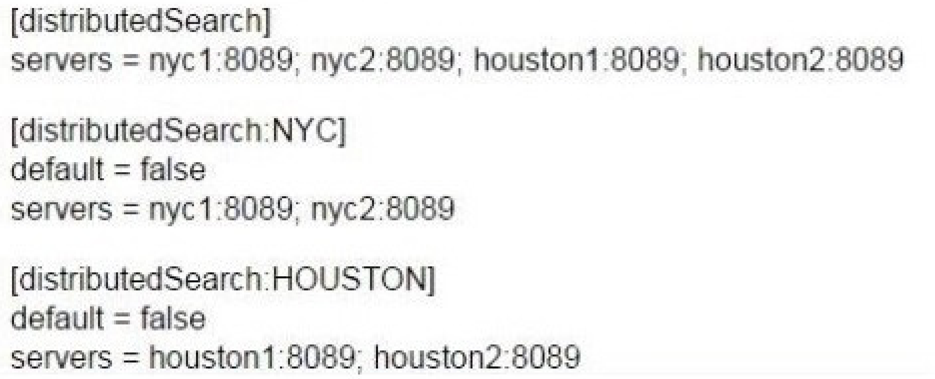
```
[distributedSearch]
servers = nyc1, nyc2, houston1, houston2

[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

Correct Answer: C
Explanation

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

QUESTION 56

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/

Correct Answer: B
Explanation

Explanation/Reference:
The correct answer is B. The network input in Splunk might be found in the $SPLUNK_HOME/etc/apps/$appName/local/inputs.conf file. A network input is a type of input that monitors data from TCP or UDP ports. To configure a network input, you need to specify the port number, the connection host, the source, and the sourcetype in the inputs.conf file.You can also set other optional settings, such as index, queue, and host_regex1. The inputs.conf file is a configuration file that contains the settings for different types of inputs, such as files, directories, scripts, network ports, and Windows event logs. The inputs.conf file can be located in various directories, depending on the scope and priority of the settings. The most common locations are:
$SPLUNK_HOME/etc/system/default: This directory contains the default settings for all inputs.You should not modify or copy the files in this directory2. $SPLUNK_HOME/etc/system/local: This directory contains the custom settings for all inputs that apply to the entire Splunk instance.The settings in this directory override the default settings2.
$SPLUNK_HOME/etc/apps/$appName/default: This directory contains the default settings for all inputs that are specific to an app.You should not modify or copy the files in this directory2. $SPLUNK_HOME/etc/apps/$appName/local: This directory contains the custom settings for all inputs that are specific to an app.The settings in this directory override the default and system settings2. Therefore, the best practice is to create or edit the inputs.conf file in the $SPLUNK_HOME/etc/apps/$appName/local directory, where $appName is the name of the app that you want to configure the network input for. This way, you can avoid modifying the default files and ensure that your settings are applied to the specific app.
The other options are incorrect because:
A. There is no network directory under the apps directory. The network input settings should be in the inputs.conf file, not in a separate directory. C. There is no udp.conf file in Splunk. The network input settings should be in the inputs.conf file, not in a separate file. The system directory is not the recommended location for custom settings, as it affects the entire Splunk instance. D. The var/lib/splunk directory is where Splunk stores the indexed data, not the input settings. The homePath setting is used to specify the location of the index data, not the input data. The inputName is not a valid variable for inputs.conf.

QUESTION 57
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: C
Explanation

Explanation/Reference:
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 58
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
Explanation

Explanation/Reference:
Hot/warm/cold/thawed bucket types are searchable. Frozen isn't searchable because its either deleted at that state or archived.

QUESTION 59
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

Correct Answer: A
Explanation

Explanation/Reference:
The correct answer is A. splunk add one shot / opt/ incident [data . log --index incident According to the Splunk documentation1, the splunk add one shot command adds a single file or directory to the Splunk index and then stops monitoring it.
This is useful for ingesting static files that do not change or update. The command takes the following syntax:
splunk add one shot <file> -index <index_name>
The file parameter specifies the path to the file or directory to be indexed. The index parameter specifies the name of the index where the data will be stored. If the index does not exist, Splunk will create it automatically. Option B is incorrect because the splunk edit monitor command modifies an existing monitor input, which is used for ingesting files or directories that change or update over time. This command does not create a new monitor input, nor does it stop monitoring after indexing.
Option C is incorrect because the splunk add monitor command creates a new monitor input, which is also used for ingesting files or directories that change or update over time. This command does not stop monitoring after indexing. Option D is incorrect because the splunk edit oneshot command does not exist. There is no such command in the Splunk CLI.
References:1:Monitor files and directories with inputs.conf - Splunk Documentation

QUESTION 60
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.

Correct Answer: C
Explanation

Explanation/Reference:
https://docs.splunk.com/Documentation/Splunk/8.1.2/Admin/Aboutlicenseviolations "An Enterprise license stack with a license volume of 100 GB of data per day or more does not currently violate."

QUESTION 61
Which Splunk component requires a Forwarder license?

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

Correct Answer: B
Explanation

QUESTION 62
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.

Correct Answer: C
Explanation

Explanation/Reference:
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.

IT TRAINER
@CERTVIP