Splunk.SPLK-1003.v2023-03-28.q103

Exam Code:	SPLK-1003
Exam Name:	Splunk Enterprise Certified Admin
Certification Provider:	Splunk
Free Question Number:	103
Version:	v2023-03-28
# of views:	1740
# of Questions views:	7397
https://www.dumpsfiles.com/files/Splunk/SPLK-1003/Splunk.SPLK-1003.v2023-03-28.q103	

NEW QUESTION: 1
Where are license files stored?
A. $SPLUNK_HOME/etc/secure
B. $SPLUNK_HOME/etc/system
C. $SPLUNK_HOME/etc/licenses
D. $SPLUNK_HOME/etc/apps/licenses
Answer: C (LEAVE A REPLY)
Explanation/Reference: https://docs.splunk.com/Documentation/Splunk/7.3.1/Admin/LicenserCLIcommands

NEW QUESTION: 2
You update a props.conffile while Splunk is running. You do not restart Splunk and you run this command:
splunk btool props list --debug. What will the output be?
A. A list of all the configurations on-disk that Splunk contains.
B. A verbose list of all configurations as they were when splunkd started.
C. A list of props.confconfigurations as they are on-disk along with a file path from which the configuration is located.
D. A list of the current running props.confconfigurations along with a file path from which the configuration was made.
Answer: D (LEAVE A REPLY)
Explanation/Reference: https://answers.splunk.com/answers/494219/need-help-with-what-should-be-a-simple- precedence.html

NEW QUESTION: 3
Using the CLI on the forwarder, how could the current forwarder to indexer configuration be viewed?
A. splunk list forward-indexer
B. splunk btool indexes list --debug
C. splunk btool server list --debug
D. splunk list forward-server
Answer: D (LEAVE A REPLY)

NEW QUESTION: 4

Consider the following stanza in inputs.conf:

```
[script:///opt/splunk/etc/apps/search/bin/lister.sh
disabled = 0
interval = 60.0
sourcetype = lister
```

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

A. /opt/splunk/ecc/apps/search/bin/liscer.sh

B. unknown

C. liscer

D. liscer.sh

Answer: (SHOW ANSWER)

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

-Scroll down to source = <string>

*Default: the input file path

NEW QUESTION: 5

Which Splunk indexer operating system platform is supported when sending logs from a Windows universal forwarder?

A. Any OS platform

B. Linux platform only

C. Windows platform only.

D. None of the above.

Answer: (SHOW ANSWER)

NEW QUESTION: 6

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

Answer: D (LEAVE A REPLY)

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.

NEW QUESTION: 7
Which is a valid stanza for a network input?
[udp://172.16.10.1:9997]
A. connection = dns
sourcetype = dns
[any://172.16.10.1:10001]
B. connection_host = ip
sourcetype = web
[tcp://172.16.10.1:9997]
C. connection_host = web
sourcetype = web
[tcp://172.16.10.1:10001]
D. connection_host = dns
sourcetype = dns
Answer: (SHOW ANSWER)
Explanation/Reference: https://docs.splunk.com/Documentation/SplunkCloud/8.0.2006/Data/ Bypassautomaticsourcetypeassignment

NEW QUESTION: 8
In which phase of the index time process does the license metering occur?
A. input phase
B. Licensing phase
C. Indexing phase
D. Parsing phase
Answer: C (LEAVE A REPLY)

NEW QUESTION: 9
The LINE_BREAKER attribute is configured in which configuration file?
A. transforms.conf
B. props.conf
C. indexes.conf
D. inpucs.conf
Answer: (SHOW ANSWER)

NEW QUESTION: 10
User role inheritance allows what to be inherited from the parent role? (Select all that apply.)
A. Parents
B. Capabilities
C. Index access

D. Search history
Answer: B (LEAVE A REPLY)
Explanation/Reference: https://docs.splunk.com/Documentation/Splunk/7.3.1/Security/ Aboutusersandroles#How_users_inherit_capabilities

NEW QUESTION: 11
The priority of layered Splunk configuration files depends on the file's:
A. Weight
B. Creation time
C. Owner
D. Context
Answer: D (LEAVE A REPLY)

NEW QUESTION: 12
The Splunk administrator wants to ensure data is distributed evenly amongst the indexers. To do this, he runs the following search over the last 24 hours:
index=*
What field can the administrator check to see the data distribution?
A. host
B. index
C. linecount
D. splunk_server
Answer: (SHOW ANSWER)
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

NEW QUESTION: 13
Which Splunk component distributes apps and certain other configuration updates to search head cluster members?
A. Deployer
B. Cluster master
C. Deployment server
D. Search head cluster master
Answer: (SHOW ANSWER)
https://docs.splunk.com/Documentation/Splunk/8.0.5/Updating/Updateconfigurations First line says it all: "The deployment server distributes deployment apps to clients."

NEW QUESTION: 14
What is required when adding a native user to Splunk? (select all that apply)
A. Default app
B. Password
C. Username

D. Full Name
Answer: (SHOW ANSWER)

NEW QUESTION: 15
Which layers are involved in Splunk configuration file layering? (select all that apply)
A. App context
B. User context
C. Forwarder context
D. Global context
Answer: A,B (LEAVE A REPLY)

NEW QUESTION: 16
Which configuration files are used to transform raw data ingested by Splunk? (Choose all that apply.)
A. props.conf
B. inputs.conf
C. rawdata.conf
D. transforms.conf
Answer: (SHOW ANSWER)
Explanation
Explanation/Reference: https://docs.splunk.com/Documentation/Splunk/8.0.5/Data/Configuretimestamprecognition

Valid SPLK-1003 Dumps shared by TrainingDump.com for Helping Passing SPLK-1003 Exam! TrainingDump.com now offer the **newest SPLK-1003 exam dumps**, the TrainingDump.com SPLK-1003 exam **questions have been updated** and **answers have been corrected** get the **newest** TrainingDump.com SPLK-1003 dumps with Test Engine here: https://www.trainingdump.com/Splunk/SPLK-1003-practice-exam-dumps.html (**203** Q&As Dumps, **40%OFF** **Special Discount:** **Exam-Tests**)

NEW QUESTION: 17
Which valid bucket types are searchable? (select all that apply)
A. Cold buckets
B. Warm buckets
C. Frozen buckets
D. Hot buckets
Answer: A,B,D (LEAVE A REPLY)

NEW QUESTION: 18
Which of the following are methods for adding inputs in Splunk? (select all that apply)
A. CLI
B. Splunk Web
C. Editing inputs. conf

D. Editing monitor. conf
Answer: A,B,C (LEAVE A REPLY)
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.

NEW QUESTION: 19
When deploying apps, which attribute in the forwarder management interface determines the apps that clients install?
A. App Class
B. Client Class
C. Server Class
D. Forwarder Class
Answer: C (LEAVE A REPLY)
Explanation/Reference: https://docs.splunk.com/Documentation/Splunk/7.3.1/Updating/Createdeploymentapps

NEW QUESTION: 20
Which optional configuration setting in inputs .conf allows you to selectively forward the data to specific indexer(s)?
A. _INDEXER_GROUP
B. _INDEXER ROUTING
C. _TCP_ROUTING
D. _INDEXER_LIST
Answer: C (LEAVE A REPLY)

NEW QUESTION: 21
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. 60 days
B. 14 days
C. 90 days
D. 7 days
Answer: A (LEAVE A REPLY)

NEW QUESTION: 22
When configuring monitor inputs with whitelists or blacklists, what is the supported method of filtering the lists?
A. Slash notation
B. Regular expression
C. Irregular expression
D. Wildcard-only expression
Answer: B (LEAVE A REPLY)
https://docs.splunk.com/Documentation/Splunk/latest/Data/Whitelistorblacklistspecificincomingdata#Include_or_exclude_specific_incoming_data

NEW QUESTION: 23
What happens when the same username exists in Splunk as well as through LDAP?
A. Splunk user is automatically deleted from authentication.conf.
B. Splunk settings take precedence.
C. LDAP user is automatically deleted from authentication.conf
D. LDAP settings take precedence.
Answer: (SHOW ANSWER)

NEW QUESTION: 24
For single line event sourcetypes. it is most efficient to set SHOULD_linemerge to what value?
A. <regex string>
B. False
C. Newline Character
D. True
Answer: B (LEAVE A REPLY)

NEW QUESTION: 25
Local user accounts created in Splunk store passwords in which file?
A. $ SFLUNK_HOME/etc/passwd
B. $ SFLUNK_HOME/etc/authentication
C. $ S?LUNK_HOME/etc/users/passwd.conf
D. $ SPLUNK HOME/etc/users/authentication.conf
Answer: A (LEAVE A REPLY)
Per the provided reference URL https://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."

NEW QUESTION: 26
What type of data is counted against the Enterprise license at a fixed 150 bytes per event?
A. License data
B. Metrics data
C. Internal Splunk data
D. Internal Windows logs
Answer: B (LEAVE A REPLY)
Explanation/Reference: https://answers.splunk.com/answers/581441/how-is-the-splunk-license-measured.html

NEW QUESTION: 27
If an update is made to an attribute in inputs.conf on a universal forwarder, on which Splunk component would the fishbucket need to be reset in order to reindex the data?
A. Indexer

B. Forwarder
C. Search head
D. Deployment server
Answer: A (LEAVE A REPLY)
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

NEW QUESTION: 28
Which of the following are supported configuration methods to add inputs on a forwarder? (Select all that apply.)
A. CLI
B. Edit inputs.conf
C. Edit forwarder.conf
D. Forwarder Management
Answer: (SHOW ANSWER)
Explanation/Reference: https://docs.splunk.com/Documentation/Forwarder/7.3.1/Forwarder/Configuretheuniversalforwarder

NEW QUESTION: 29
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 D
B. Option B
C. option A
D. Option C
Answer: A (LEAVE A REPLY)

NEW QUESTION: 30
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. ignore = 45d
B. ignoreOlderThan = 45d
C. followTail = -45d
D. includeNewerThan = -35d
Answer: B (LEAVE A REPLY)

NEW QUESTION: 31
After an Enterprise Trial license expires, it will automatically convert to a Free license. How many days is an Enterprise Trial license valid before this conversion occurs?
A. 90 days
B. 60 days
C. 7 days
D. 14 days
Answer: B (LEAVE A REPLY)
Reference:
https://docs.splunk.com/Documentation/Splunk/8.2.3/Admin/TypesofSplunklicenses

Valid SPLK-1003 Dumps shared by TrainingDump.com for Helping Passing SPLK-1003 Exam! TrainingDump.com now offer the **newest SPLK-1003 exam dumps**, the TrainingDump.com SPLK-1003 exam **questions have been updated** and **answers have been corrected** get the **newest** TrainingDump.com SPLK-1003 dumps with Test Engine here: https://www.trainingdump.com/Splunk/SPLK-1003-practice-exam-dumps.html (**203** Q&As Dumps, **40%OFF** **Special Discount:** **Exam-Tests**)

NEW QUESTION: 32
When running a real-time search, search results are pulled from which Splunk component?
A. Heavy forwarders and search peers
B. Heavy forwarders
C. Search heads
D. Search peers
Answer: (SHOW ANSWER)
Using the Splunk reference URL https://docs.splunk.com/Splexicon:Searchpeer
"search peer is a splunk platform instance that responds to search requests from a search head. The term "search peer" is usally synonymous with the indexer role in a distributed search topology. However, other instance types also have access to indexed data, particularly internal diagnostic data, and thus function as search peers when they respond to search requests for that data."

NEW QUESTION: 33

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

A. Use Local Windows host monitoring.

B. Use Windows Remote Inputs with WMI.

C. Use Local Windows network monitoring.

D. Use an index with an Index Data Type of Metrics.

Answer: B (LEAVE A REPLY)

https://docs.splunk.com/Documentation/Splunk/8.1.0/Data/ConsiderationsfordecidinghowtomonitorWindowsdata

"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."

NEW QUESTION: 34

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

A. $SPLUNK_HOME/etc/passwd

B. $SPLUNK_HOME/etc/authentication

C. $SPLUNK_HOME/etc/users/passwd.conf

D. $SPLUNK_HOME/etc/users/authentication.conf

Answer: A (LEAVE A REPLY)

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

NEW QUESTION: 35

Which of the following are supported options when configuring optional network inputs?

A. Metadata override, sender filtering options, network input queues (quantum queues)

B. Metadata override, sender filtering options, network input queues (memory/persistent queues)

C. Filename override, sender filtering options, network output queues (memory/persistent queues)

D. Metadata override, receiver filtering options, network input queues (memory/persistent queues)

Answer: B (LEAVE A REPLY)

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

NEW QUESTION: 36

Which Splunk indexer operating system platform is supported when sending logs from a Windows universal forwarder?

A. Any OS platform.

B. Linux platform only.

C. Windows platform only.

D. None of the above.

Answer: (SHOW ANSWER)

Explanation/Reference:

https://docs.splunk.com/Documentation/Splunk/7.3.2/Installation/Systemrequirements#Supported_OSes

NEW QUESTION: 37

When does a warm bucket roll over to a cold bucket?
A. When Splunk is restarted.
B. When the maximum warm bucket age has been reached.
C. When the maximum warm bucket size has been reached.
D. When the maximum number of warm buckets is reached.
Answer: D (LEAVE A REPLY)
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 always selects 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:
166653

NEW QUESTION: 38
Which of the following accurately describes HTTP Event Collector indexer acknowledgement?
A. It can be enabled at the global setting level.
B. It stores status information on the Splunk server.
C. It is configured the same as indexer acknowledgement used to protect in-flight data.
D. It requires a separate channel provided by the client.
Answer: A (LEAVE A REPLY)

NEW QUESTION: 39
Which Splunk component distributes apps and certain other configuration updates to search head cluster members?
A. Search head cluster master
B. Cluster master
C. Deployment server
D. Deployer
Answer: D (LEAVE A REPLY)

NEW QUESTION: 40
Where are deployment server apps mapped to clients?
A. Apps tab in forwarder management interface or clientapps.conf.
B. Clients tab in forwarder management interface or deploymentclient.conf.
C. Server Classes tab in forwarder management interface or serverclass.conf.
D. Client Applications tab in forwarder management interface or clientapps.conf.
Answer: C (LEAVE A REPLY)
Reference:
Updateconfigurations#2._Reload_the_deployment_server
https://docs.splunk.com/Documentation/Splunk/8.0.5/Updating/Useserverclass.conf
"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."

NEW QUESTION: 41
An index stores its data in buckets. Which default directories does Splunk use to store buckets? (Choose all that apply.)
A. bucketdb
B. colddb
C. frozendb
D. db
Answer: B,C (LEAVE A REPLY)

NEW QUESTION: 42
When using license pools, volume allocations apply to which Splunk components?
A. Heavy Forwarders
B. Indexers
C. Indexes
D. Search Heads
Answer: (SHOW ANSWER)

NEW QUESTION: 43
Which of the following configuration files are used with a universal forwarder? (Choose all that apply.)
A. inputs.conf
B. monitor.conf
C. outputs.conf
D. forwarder.conf
Answer: (SHOW ANSWER)
Reference:
Configuretheuniversalforwarder

NEW QUESTION: 44
What is the correct order of steps in Duo Multifactor Authentication?
A. 1. Request Login 2 Duo MFA
3. Authentication Granted 4 Connect to SAML server
5. Log into Splunk
6. Create User session
B. 1 Request Login
2 Check authentication / group mapping
3 Authentication Granted
4. Duo MFA
5. Create User session
6. Log into Splunk
C. 1 Request Login
2. Connect to SAML server

3 Duo MFA
4 Create User session
5 Authentication Granted 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
Answer: B (LEAVE A REPLY)

NEW QUESTION: 45
Which of the following statements describe deployment management? (select all that apply)
A. Requires an Enterprise license
B. Is responsible for sending apps to forwarders.
C. Once used, is the only way to manage forwarders
D. Can automatically restart the host OS running the forwarder.
Answer: (SHOW ANSWER)
https://docs.splunk.com/Documentation/Splunk/8.2.2/Admin/Distdeploylicenses#:~:text=License%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."

NEW QUESTION: 46
Which Splunk indexer operating system platform is supported when sending logs from a Windows universal forwarder?
A. Any OS platform
B. Linux platform only
C. Windows platform only.
D. None of the above.
Answer: A (LEAVE A REPLY)
"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.

Valid SPLK-1003 Dumps shared by TrainingDump.com for Helping Passing SPLK-1003 Exam! TrainingDump.com now offer the **newest SPLK-1003 exam dumps**, the TrainingDump.com SPLK-1003 exam **questions have been updated** and **answers have been corrected** get the **newest** TrainingDump.com SPLK-1003 dumps with Test Engine here: https://www.trainingdump.com/Splunk/SPLK-1003-practice-exam-dumps.html (**203** Q&As Dumps, **40%OFF** **Special Discount:** **Exam-Tests**)

NEW 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. Search
B. Data preview
C. Apps
D. Forwarder inputs
Answer: A (LEAVE A REPLY)

NEW QUESTION: 48
How does the Monitoring Console monitor forwarders?
A. By pulling internal logs from forwarders.
B. By using the forwarder monitoring add-on
C. With internal logs forwarded by forwarders.
D. With internal logs forwarded by deployment server.
Answer: C (LEAVE A REPLY)
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."

NEW QUESTION: 49
Which layers are involved in Splunk configuration file layering? (Choose all that apply.)
A. Global context
B. App context
C. Forwarder context
D. User context
Answer: A,B,D (LEAVE A REPLY)

NEW QUESTION: 50
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
Answer: B (LEAVE A REPLY)
Reference:
433035

NEW QUESTION: 51
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
```

dumpsfiles.com splunk>

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 TIMESTAMP LOOKAHEAD - 30
D. MAX_TIMESTAMF_LOOKHEAD = 20
Answer: (SHOW ANSWER)

NEW QUESTION: 52
Which of the following is a valid distributed search group?
[distributedSearch:Paris]
A. default = false
servers = server1, server2
B. [searchGroup:Paris]
default = false
servers = server1:8089, server2:8089
[searchGroup:Paris]
C. default = false
servers = server1:9997, server2:9997

[distributedSearch:Paris]
D. default = false
servers = server1:8089; server2:8089
Answer: D (LEAVE A REPLY)
Explanation/Reference: https://docs.splunk.com/Documentation/Splunk/7.3.1/DistSearch/Distributedsearchgroups

NEW QUESTION: 53
During search time, which directory of configuration files has the highest precedence?
A. $SFLUNK_KOME/etc/system/local
B. $SPLUNK_KCME/etc/system/default
C. $SPLUNK_HCME/etc/apps/app1/local
D. $SPLUNK HCME/etc/users/admin/local
Answer: D (LEAVE A REPLY)
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

NEW QUESTION: 54
Which Splunk component does a search head primarily communicate with?
A. Deployment server
B. Indexer
C. Cluster master
D. Forwarder
Answer: B (LEAVE A REPLY)

NEW QUESTION: 55
What is the valid option for a [monitor] stanza in inputs.conf?
A. ignoreOlderThan
B. enabled
C. datasource
D. server_name
Answer: A (LEAVE A REPLY)

NEW QUESTION: 56

In a distributed environment, which Splunk component is used to distribute apps and configurations to the other Splunk instances?
A. Deployment server
B. Deployer
C. Forwarder
D. Indexer
Answer: A (LEAVE A REPLY)

NEW QUESTION: 57
Which Splunk forwarder has a built-in license?
A. Heavy forwarder
B. Cloud forwarder
C. Universal forwarder
D. Light forwarder
Answer: C (LEAVE A REPLY)

NEW QUESTION: 58
What type of data is counted against the Enterprise license at a fixed 150 bytes per event?
A. License data
B. Internal Splunk data
C. Internal Windows logs
D. Metricsdata
Answer: D (LEAVE A REPLY)

NEW QUESTION: 59
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

Answer: C (LEAVE A REPLY)

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

NEW QUESTION: 60

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

Answer: A (LEAVE A REPLY)

NEW QUESTION: 61

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

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

Answer: C (LEAVE A REPLY)

Valid SPLK-1003 Dumps shared by TrainingDump.com for Helping Passing SPLK-1003 Exam! TrainingDump.com now offer the **newest SPLK-1003 exam dumps**, the TrainingDump.com SPLK-1003 exam **questions have been updated** and **answers have been corrected** get the **newest** TrainingDump.com SPLK-1003 dumps with Test Engine here: https://www.trainingdump.com/Splunk/SPLK-1003-practice-exam-dumps.html (**203** Q&As Dumps, **40%OFF** **Special Discount:** **Exam-Tests**)

NEW QUESTION: 62

Which of the following are supported configuration methods to add inputs on a forwarder? (select all that apply)

A. CLI
B. Edit inputs . conf
C. Edit forwarder.conf

D. Forwarder Management
Answer: A,B,D (LEAVE A REPLY)
https://docs.splunk.com/Documentation/Forwarder/8.2.1/Forwarder/HowtoforwarddatatoSplunkEnterprise
"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

NEW QUESTION: 63
How do you remove missing forwarders from the Monitoring Console?
A. By reloading the deployment server.
B. By rescanning active forwarders.
C. By rebuilding the forwarder asset table.
D. By restarting Splunk.
Answer: B (LEAVE A REPLY)

NEW QUESTION: 64
When does a warm bucket roll over to a cold bucket?
A. When the maximum number of warm buckets is reached.
B. When the maximum warm bucket age has been reached.
C. When the maximum warm bucket size has been reached.
D. When Splunk is restarted.
Answer: A (LEAVE A REPLY)

NEW QUESTION: 65
All search-time field extractions should be specified on which Splunk component?
A. Indexer
B. Search head
C. Universal forwarder
D. Deployment server
Answer: (SHOW ANSWER)

NEW QUESTION: 66
What is the difference between the two wildcards ... and - for the monitor stanza in inputs, conf?
A. ... is not supported in monitor stanzas
B. There is no difference, they are interchangable and match anything beyond directory boundaries.
C. * matches anything in that specific directory path segment, whereas ... recurses through subdirectories as well.
D. ... matches anything in that specific directory path segment, whereas - recurses through subdirectories as well.
Answer: C (LEAVE A REPLY)
https://docs.splunk.com/Documentation/Splunk/7.3.0/Data/Specifyinputpathswithwildcards

... 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.

NEW QUESTION: 67
You update a props. conf file while Splunk is running. You do not restart Splunk and you run this command: splunk btoo1 props list -debug.
What will the output be?
A. list of all the configurations on-disk that Splunk contains.
B. A verbose list of all configurations as they were when splunkd started.
C. A list of props. conf configurations as they are on-disk along with a file path from which the configuration is located
D. A list of the current running props, conf configurations along with a file path from which the configuration was made
Answer: C (LEAVE A REPLY)
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."

NEW QUESTION: 68
Which of the following statements describe deployment management? (select all that apply)
A. Once used, is the only way to manage forwarders
B. Can automatically restart the host OS running the forwarder.
C. Is responsible for sending apps to forwarders.
D. Requires an Enterprise license
Answer: D (LEAVE A REPLY)

NEW QUESTION: 69
Which Splunk component does a search head primarily communicate with?
A. Indexer
B. Forwarder
C. Deployment server
D. Cluster master
Answer: C (LEAVE A REPLY)

NEW QUESTION: 70
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)



B)



C)



D)



A. option A

B. Option B

C. Option C

D. Option D

Answer: C (LEAVE A REPLY)

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

NEW QUESTION: 71
Which of the following are methods for adding inputs in Splunk? (select all that apply)
A. Editing inputs. conf
B. Editing monitor. conf
C. CLI
D. Splunk Web
Answer: D (LEAVE A REPLY)

NEW QUESTION: 72
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 D
B. Option C
C. option A
D. Option B
Answer: C (LEAVE A REPLY)

NEW QUESTION: 73
Which configuration files are used to transform raw data ingested by Splunk? (Choose all that apply.)
A. props.conf
B. rawdata.conf
C. transforms.conf
D. inputs.conf
Answer: A (LEAVE A REPLY)

NEW QUESTION: 74
What are the required stanza attributes when configuring the transforms. conf to manipulate or remove events?
A. REGEX, DEST. FORMAT
B. REGEX. SRC_KEY, FORMAT
C. REGEX, DEST_KEY, FORMAT
D. REGEX, DEST_KEY FORMATTING
Answer: C (LEAVE A REPLY)
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.

NEW QUESTION: 75
What is the default character encoding used by Splunk during the input phase?
A. UTF-16
B. UTF-8
C. ISO 8859
D. EBCDIC
Answer: B (LEAVE A REPLY)

NEW QUESTION: 76
What conf file needs to be edited to set up distributed search groups?
A. props.conf
B. search.conf
C. distsearch.conf
D. distibutedsearch.conf
Answer: C (LEAVE A REPLY)
Explanation/Reference: https://docs.splunk.com/Documentation/Splunk/8.0.5/DistSearch/Distributedsearchgroups

Valid SPLK-1003 Dumps shared by TrainingDump.com for Helping Passing SPLK-1003 Exam! TrainingDump.com now offer the **newest SPLK-1003 exam dumps**, the TrainingDump.com SPLK-1003 exam **questions have been updated** and **answers have been corrected**

get the **newest** TrainingDump.com SPLK-1003 dumps with Test Engine here: https://www.trainingdump.com/Splunk/SPLK-1003-practice-exam-dumps.html (**203** Q&As Dumps, **40%OFF Special Discount: Exam-Tests**)

NEW QUESTION: 77
Which of the following are reasons to create separate indexes? (Choose all that apply.)
A. File organization.
B. Different retention times.
C. Restrict user permissions.
D. Increase number of users.
Answer: A,B (LEAVE A REPLY)

NEW QUESTION: 78
Which Splunk configuration file is used to enable data integrity checking?
A. props.conf
B. global.conf
C. indexes.conf
D. data_integrity.conf
Answer: C (LEAVE A REPLY)
https://docs.splunk.com/Documentation/Splunk/8.1.2/Security/Dataintegritycontrol#:~:text=When%20you%20enable%20data%20integrity%20control%2C%20Splunk%20Enterprise%20computes%20hashes,it%20to%20a%20l1Hashes%20file.

NEW QUESTION: 79
How is data handled by Splunk during the input phase of the data ingestion process?
A. Data is treated as streams.
B. Data is broken up into events.
C. Data is initially written to disk.
D. Data is measured by the license meter.
Answer: C (LEAVE A REPLY)
Explanation/Reference: https://docs.splunk.com/Documentation/Splunk/8.0.5/Deploy/Datapipeline

NEW QUESTION: 80
In which Splunk configuration is the SEDCMD used?
A. props, conf
B. inputs.conf
C. indexes.conf
D. transforms.conf
Answer: A (LEAVE A REPLY)
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. "

NEW QUESTION: 81

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

A. inputs.conf

B. indexes.conf

C. outputs.conf

D. servers.conf

Answer: C (LEAVE A REPLY)

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/Configureforwardingwithoutputs.conf

NEW QUESTION: 82

The universal forwarder has which capabilities when sending data? (select all that apply)

A. Sending alerts

B. Compressing data

C. Obfuscating/hiding data

D. Indexer acknowledgement

Answer: B,D (LEAVE A REPLY)

Explanation

https://docs.splunk.com/Documentation/Splunk/8.0.1/Forwarding/Aboutforwardingandreceivingdata

NEW QUESTION: 83

Which of the following configuration files are used with a universal forwarder? (Choose all that apply.)

A. inputs.conf

B. monitor.conf

C. outputs.conf

D. forwarder.conf

Answer: A,C (LEAVE A REPLY)

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

--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:

Configuretheuniversalforwarder

NEW QUESTION: 84

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

A. $SPLUNK_HCME/etc/sear:ch

B. $SPLUNK_HCME/etc/master-apps

C. $SFLUNK_KOME/etc/apps

D. $SPLUNK HCME/etc/deployment-apps

Answer: (SHOW ANSWER)

NEW QUESTION: 85
After how many warnings within a rolling 30-day period will a license violation occur with an enforced Enterprise license?
A. 1
B. 3
C. 4
D. 5
Answer: D (LEAVE A REPLY)
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."

NEW QUESTION: 86
To set up a network input in Splunk, what needs to be specified?
A. File path.
B. Username and password.
C. Network protocol and port number.
D. Network protocol and MAC address.
Answer: A (LEAVE A REPLY)
Explanation/Reference: http://dev.splunk.com/view/dev-guide/SP-CAAAE3A

NEW QUESTION: 87
In which phase do indexed extractions in props.conf occur?
A. Inputs phase
B. Parsing phase
C. Indexing phase
D. Searching phase
Answer: B (LEAVE A REPLY)
The following items in the phases below are listed in the order Splunk applies them (ie LINE_BREAKER occurs before TRUNCATE).
Input phase
inputs.conf
props.conf
CHARSET
NO_BINARY_CHECK
CHECK_METHOD
CHECK_FOR_HEADER (deprecated)
PREFIX_SOURCETYPE
sourcetype
wmi.conf
regmon-filters.conf

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

NEW QUESTION: 88
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. none of the above
B. /var/log/messages
C. /var/log/maillog
D. /var/log/maillog and /var/log/messages
Answer: C (LEAVE A REPLY)

NEW QUESTION: 89
Which option on the Add Data menu is most useful for testing data ingestion without creating inputs.conf?
A. Download option
B. Monitor option
C. Upload option
D. Forward option
Answer: C (LEAVE A REPLY)

NEW QUESTION: 90
Which forwarder type can parse data prior to forwarding?
A. Universal forwarder
B. Heaviest forwarder
C. Hyper forwarder
D. Heavy forwarder
Answer: D (LEAVE A REPLY)
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."

NEW QUESTION: 91
For single line event sourcetypes. it is most efficient to set SHOULD_linemerge to what value?
A. True
B. False
C. <regex string>
D. Newline Character
Answer: B (LEAVE A REPLY)
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.

Valid SPLK-1003 Dumps shared by TrainingDump.com for Helping Passing SPLK-1003 Exam! TrainingDump.com now offer the **newest SPLK-1003 exam dumps**, the TrainingDump.com SPLK-1003 exam **questions have been updated** and **answers have been corrected** get the **newest** TrainingDump.com SPLK-1003 dumps with Test Engine here: https://www.trainingdump.com/Splunk/SPLK-1003-practice-exam-dumps.html (**203** Q&As Dumps, **40%OFF** **Special Discount:** **Exam-Tests**)

NEW QUESTION: 92
What are the required stanza attributes when configuring the transforms. conf to manipulate or remove events?
A. REGEX, DEST. FORMAT
B. REGEX, DEST_KEY FORMATTING
C. REGEX, DEST_KEY, FORMAT
D. REGEX. SRC_KEY, FORMAT
Answer: (SHOW ANSWER)

NEW QUESTION: 93
Which of the following types of data count against the license daily quota?
A. Replicated data
B. splunkd logs
C. Windows internal logs

D. Summary index data
Answer: B (LEAVE A REPLY)

NEW QUESTION: 94
What conf file needs to be edited to set up distributed search groups?
A. props.conf
B. search.conf
C. distsearch.conf
D. distibutedsearch.conf
Answer: C (LEAVE A REPLY)
"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"

NEW QUESTION: 95
How does the Monitoring Console monitor forwarders?
A. By using the forwarder monitoring add-on
B. By pulling internal logs from forwarders.
C. With internal logs forwarded by deployment server.
D. With internal logs forwarded by forwarders.
Answer: D (LEAVE A REPLY)

NEW QUESTION: 96
When configuring monitor inputs with whitelists or blacklists, what is the supported method of filtering the lists?
A. Wildcard-only expression
B. Slash notation
C. Irregular expression
D. Regular expression
Answer: (SHOW ANSWER)

NEW QUESTION: 97
The universal forwarder has which capabilities when sending data? (Select all that apply.)
A. Sending alerts
B. Compressing data
C. Obfuscating/hiding data
D. Indexer acknowledgement
Answer: D (LEAVE A REPLY)
Explanation/Reference: https://docs.splunk.com/Documentation/Splunk/7.3.1/Forwarding/Typesofforwarders

NEW QUESTION: 98
Assume a file is being monitored and the data was incorrectly indexed to an exclusive index. The index is cleaned and now the data must be reindexed. What other index must be cleaned to reset the input checkpoint information for that file?

A. _audit
B. _checkpoint
C. _introspection
D. _thefishbucket
Answer: (SHOW ANSWER)
--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. https://docs.splunk.com/Documentation/Splunk/8.1.1/Troubleshooting/CommandlinetoolsforusewithSupport

NEW QUESTION: 99
Where are deployment server apps mapped to clients?
A. Client Applications 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. Apps tab in forwarder management interface or clientapps.conf.
Answer: C (LEAVE A REPLY)

NEW QUESTION: 100
Which of the following are available input methods when adding a file input in Splunk Web? (Choose all that apply.)
A. Index once.
B. Monitor interval.
C. On-demand monitor.
D. Continuously monitor.
Answer: (SHOW ANSWER)
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.

NEW QUESTION: 101
What are the minimum required settings when creating a network input in Splunk?
A. Protocol, port number
B. Protocol, port, location
C. Protocol, username, port
D. Protocol, IP, port number
Answer: (SHOW ANSWER)
Explanation/Reference: https://docs.splunk.com/Documentation/Splunk/7.3.1/Data/UsetheHTTPEventCollector

NEW QUESTION: 102
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 to Active Directory
D. Map LDAP Inheritance
Answer: B (LEAVE A REPLY)

NEW QUESTION: 103
Which artifact is required in the request header when creating an HTTP event?
A. Host name
B. Token
C. Manifest
D. ackID
Answer: B (LEAVE A REPLY)

Valid SPLK-1003 Dumps shared by TrainingDump.com for Helping Passing SPLK-1003 Exam! TrainingDump.com now offer the **newest SPLK-1003 exam dumps**, the TrainingDump.com SPLK-1003 exam **questions have been updated** and **answers have been corrected** get the **newest** TrainingDump.com SPLK-1003 dumps with Test Engine here: https://www.trainingdump.com/Splunk/SPLK-1003-practice-exam-dumps.html (**203** Q&As Dumps, **40%OFF** **Special Discount:** **Exam-Tests**)