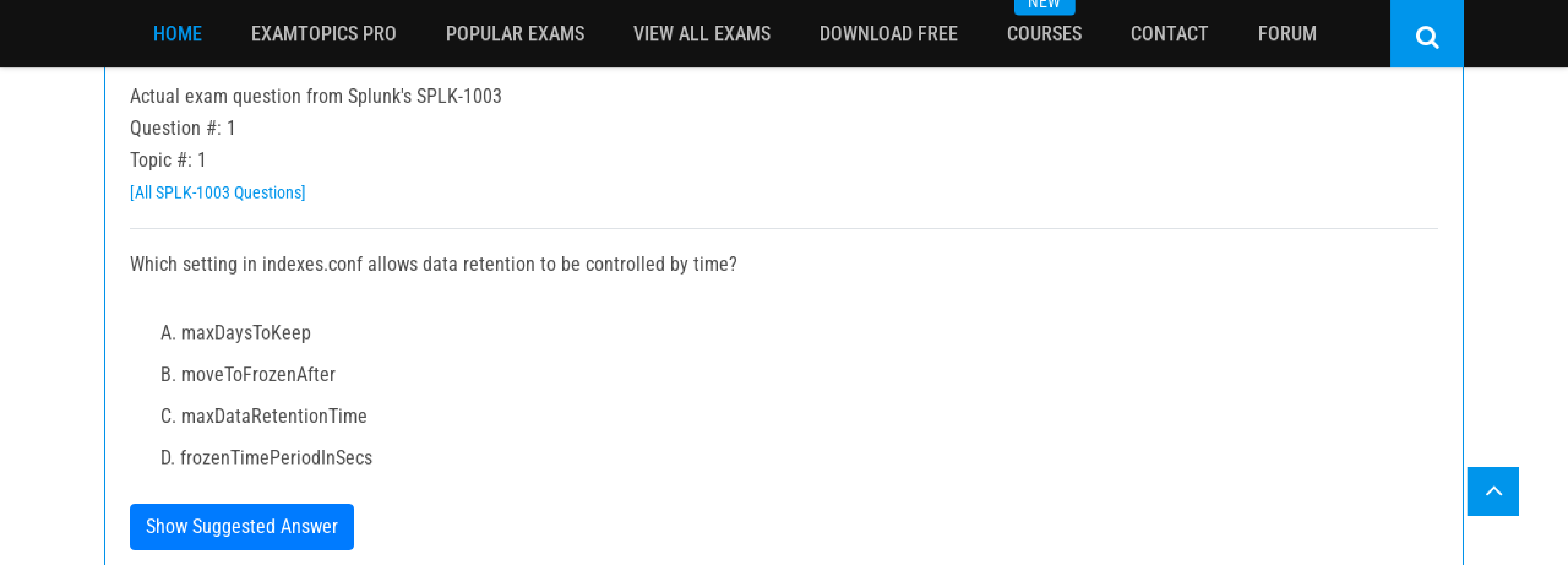


Actual exam question from Splunk's SPLK-1003

Question #: 1

Topic #: 1

[All SPLK-1003 Questions]

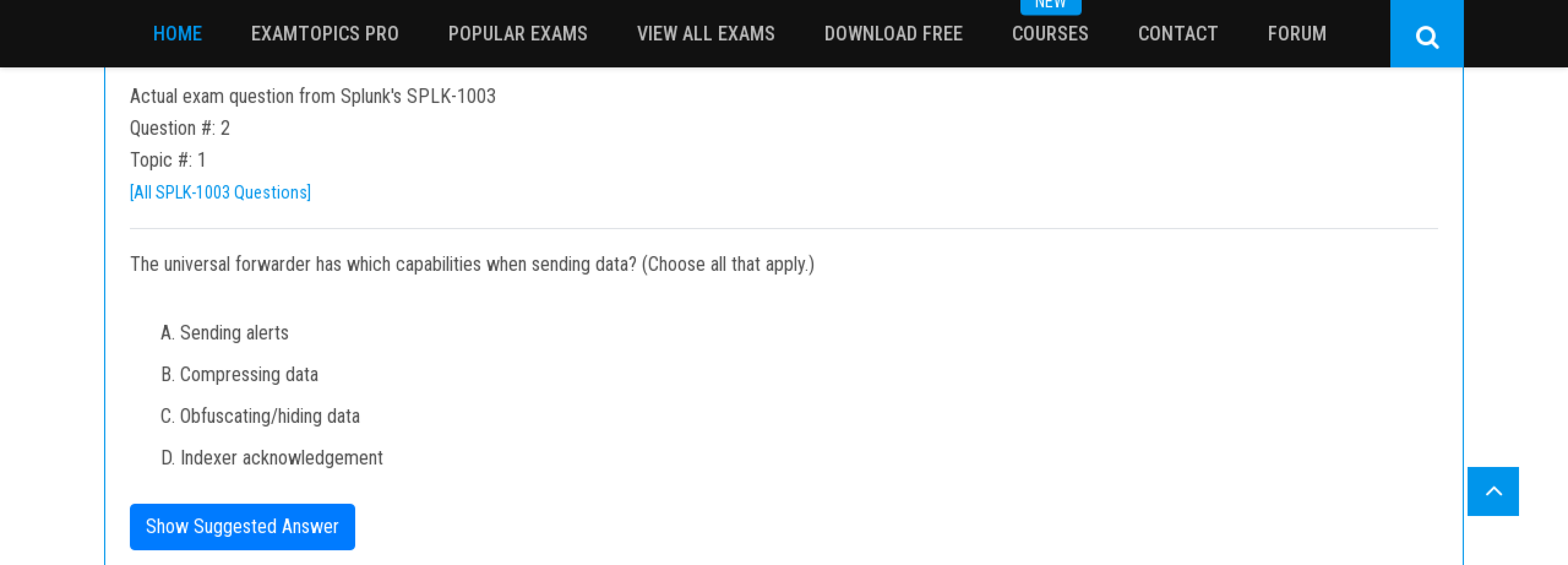
Which setting in indexes.conf allows data retention to be controlled by time?

A. maxDaysToKeep

B. moveToFrozenAfter

C. maxDataRetentionTime

D. frozenTimePeriodInSecs



Actual exam question from Splunk's SPLK-1003

Question #: 2

Topic #: 1

[All SPLK-1003 Questions]

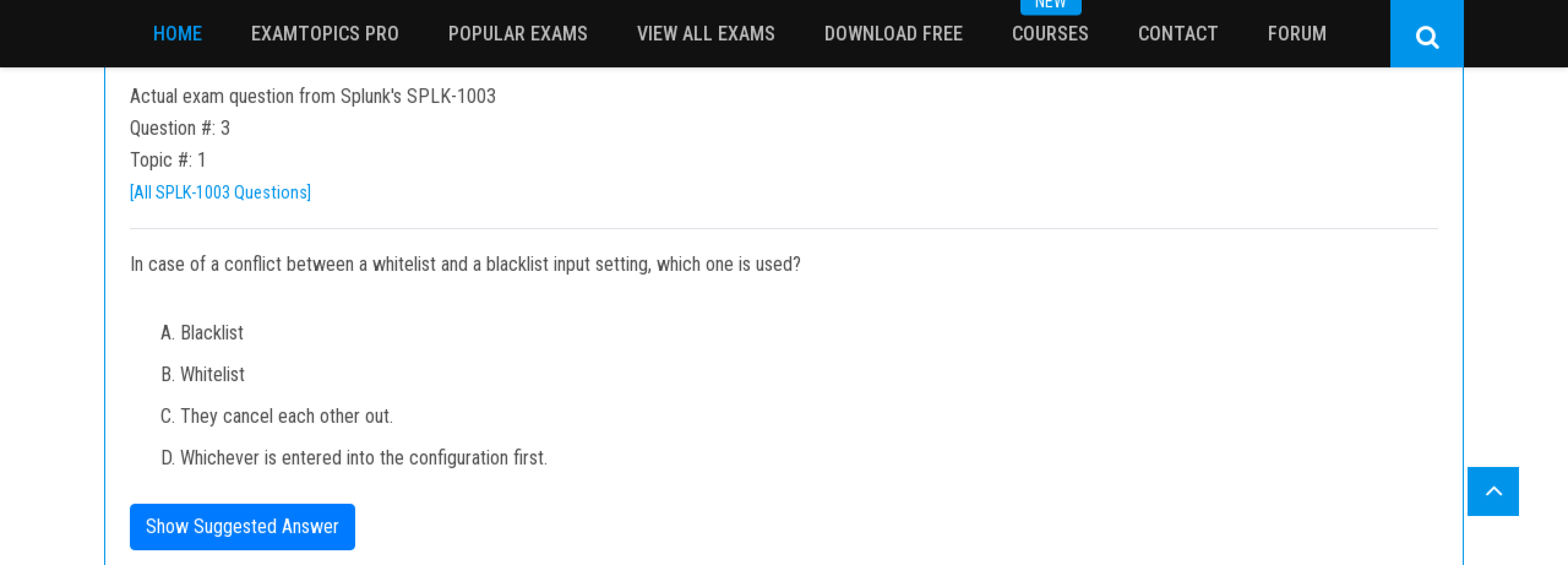
The universal forwarder has which capabilities when sending data? (Choose all that apply.)

A. Sending alerts

B. Compressing data

C. Obfuscating/hiding data

D. Indexer acknowledgement



Actual exam question from Splunk's SPLK-1003

Question #: 3

Topic #: 1

[All SPLK-1003 Questions]

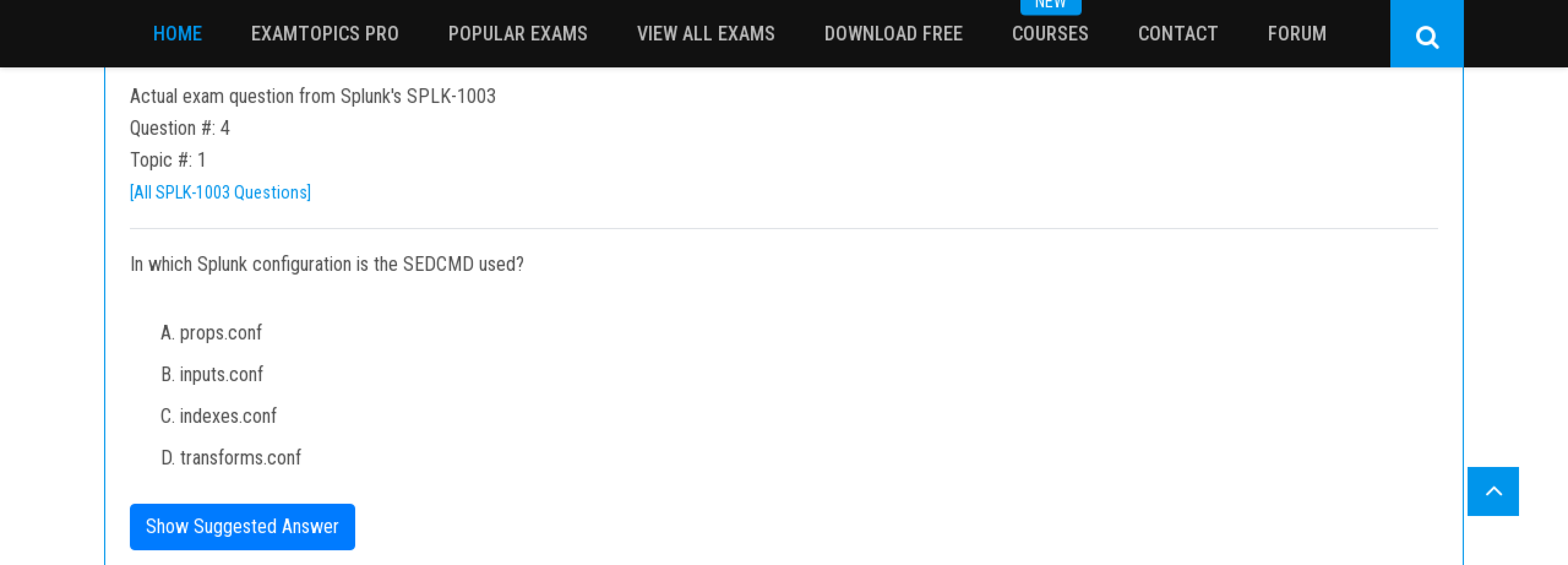
In case of a conflict between a whitelist and a blacklist input setting, which one is used?

A. Blacklist

B. Whitelist

C. They cancel each other out.

D. Whichever is entered into the configuration first.



Actual exam question from Splunk's SPLK-1003

Question #: 4

Topic #: 1

[All SPLK-1003 Questions]

In which Splunk configuration is the SEDCMD used?

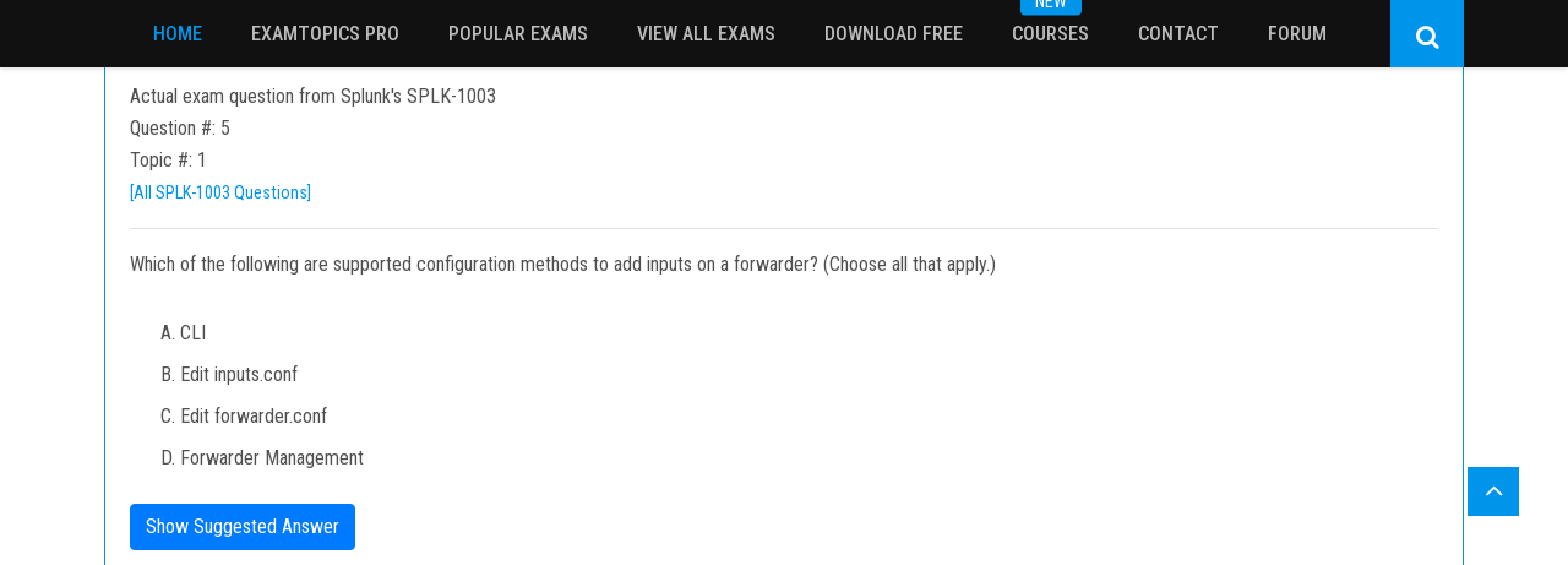
A. props.conf

B. inputs.conf

C. indexes.conf

D. transforms.conf

Show Suggested Answer



Actual exam question from Splunk's SPLK-1003

Question #: 5

Topic #: 1

[All SPLK-1003 Questions]

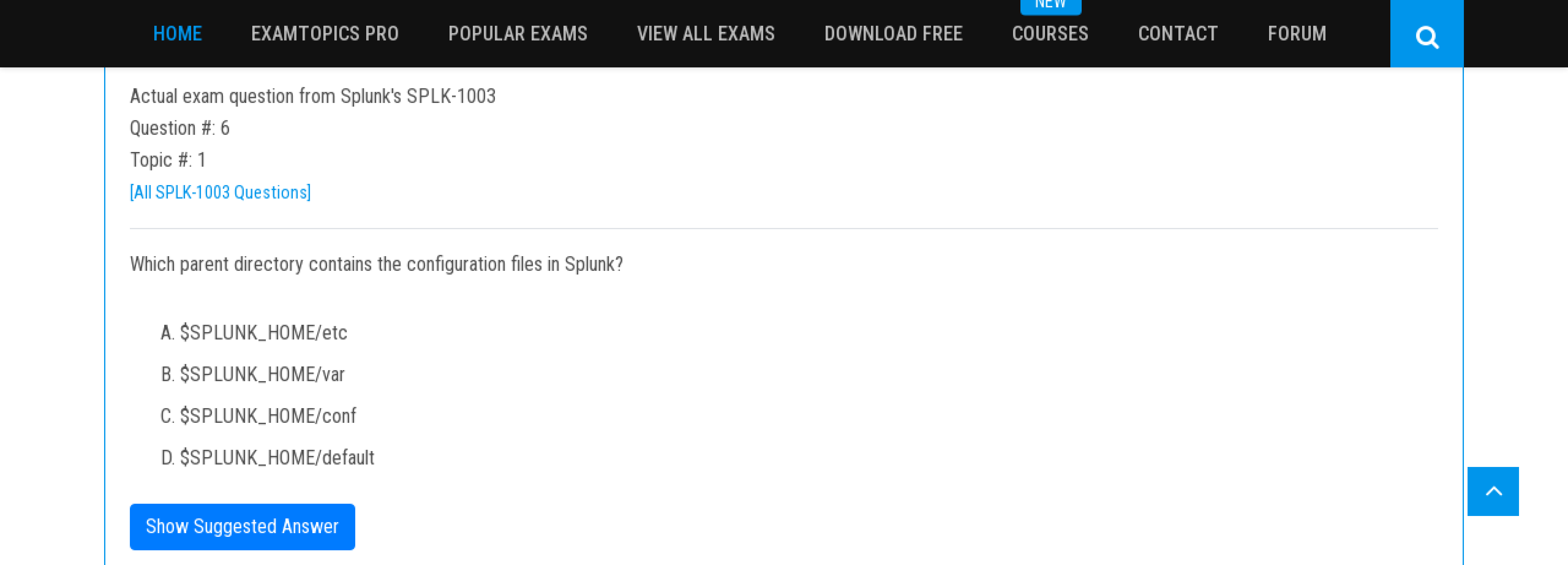
Which of the following are supported configuration methods to add inputs on a forwarder? (Choose all that apply.)

A. CLI

B. Edit inputs.conf

C. Edit forwarder.conf

D. Forwarder Management



Actual exam question from Splunk's SPLK-1003

Question #: 6

Topic #: 1

[All SPLK-1003 Questions]

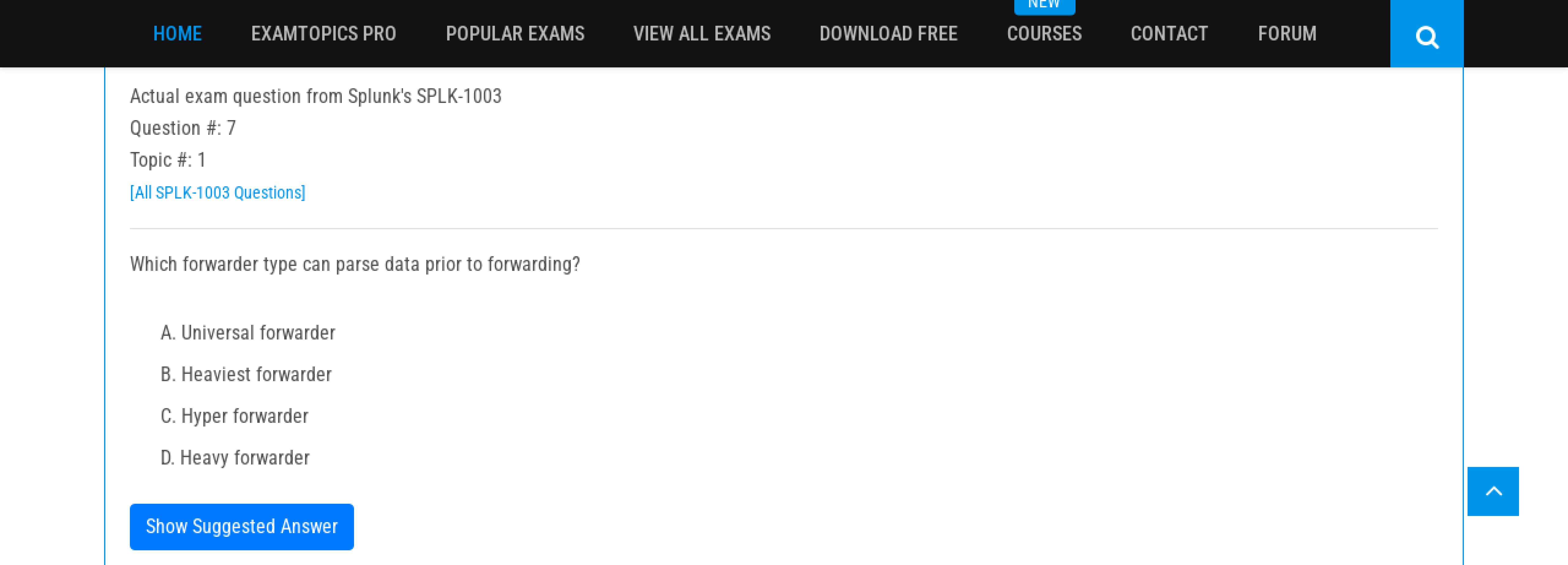
Which parent directory contains the configuration files in Splunk?

A. $SPLUNK_HOME/etc

B. $SPLUNK_HOME/var

C. $SPLUNK_HOME/conf

D. $SPLUNK_HOME/default



Actual exam question from Splunk's SPLK-1003

Question #: 7

Topic #: 1

[All SPLK-1003 Questions]

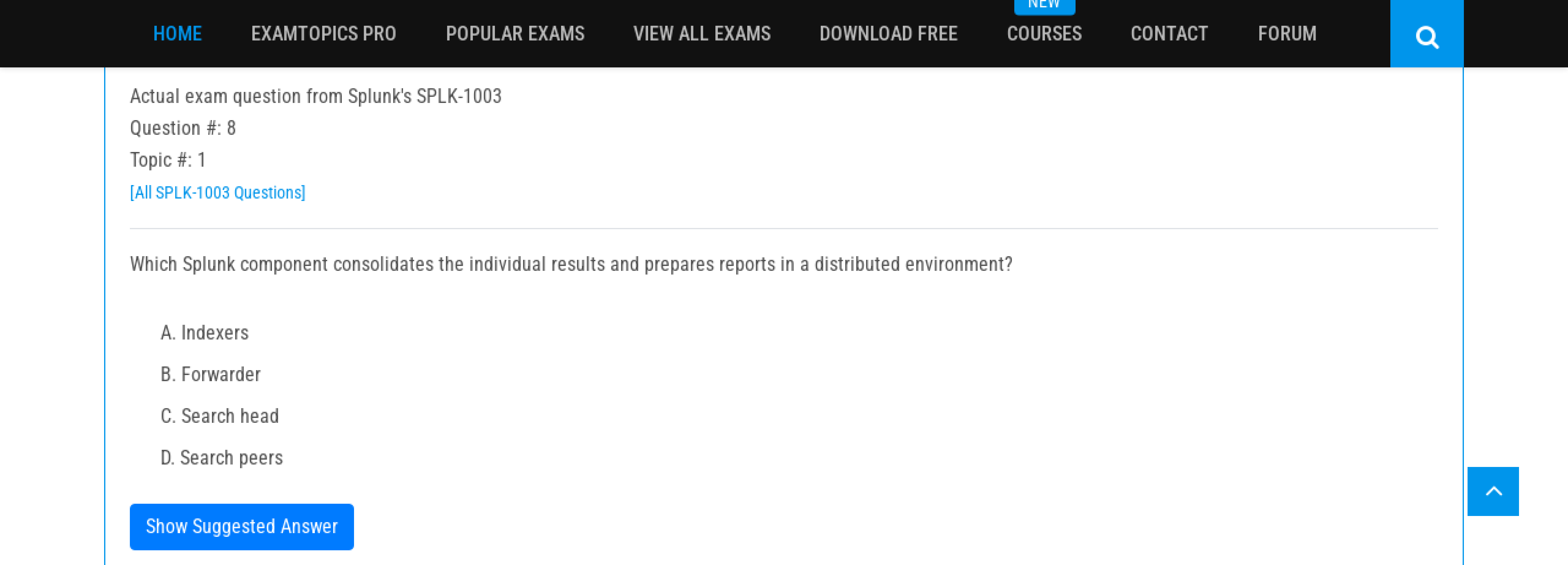
Which forwarder type can parse data prior to forwarding?

A. Universal forwarder

B. Heaviest forwarder

C. Hyper forwarder

D. Heavy forwarder



Actual exam question from Splunk's SPLK-1003

Question #: 8

Topic #: 1

[All SPLK-1003 Questions]

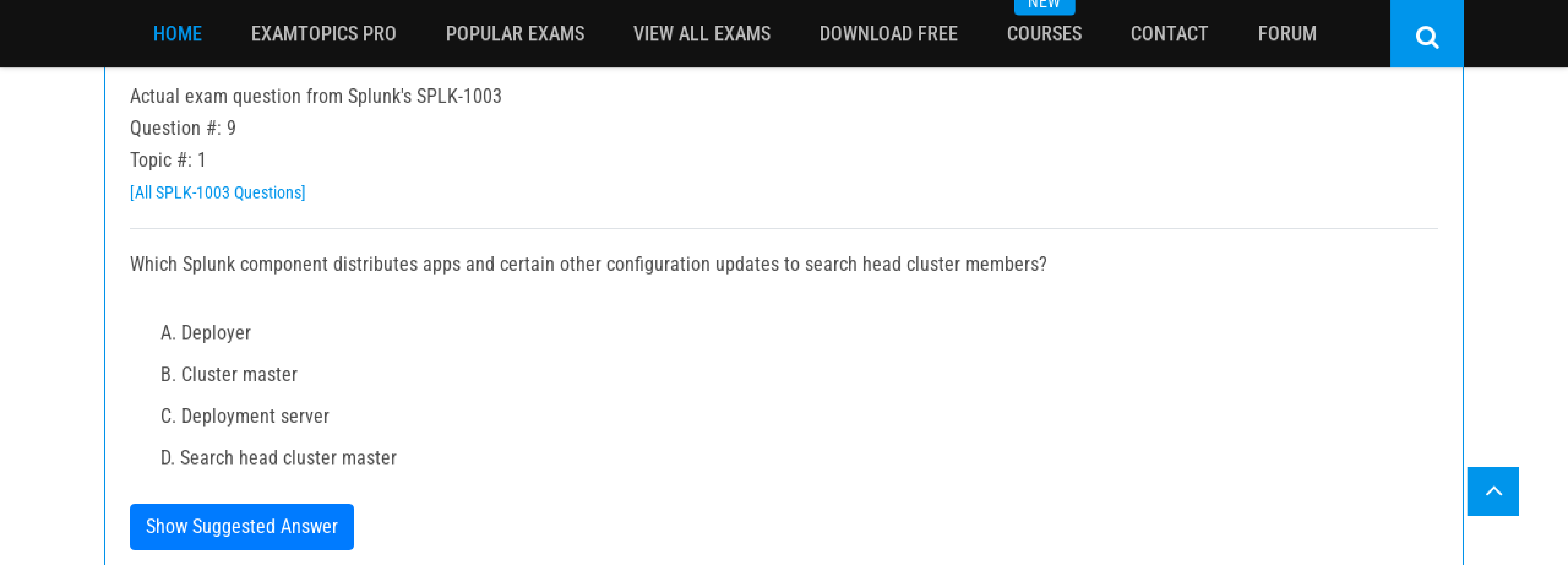
Which Splunk component consolidates the individual results and prepares reports in a distributed environment?

A. Indexers

B. Forwarder

C. Search head

D. Search peers



Actual exam question from Splunk's SPLK-1003

Question #: 9

Topic #: 1

[All SPLK-1003 Questions]

Which Splunk component distributes apps and certain other configuration updates to search head cluster members?

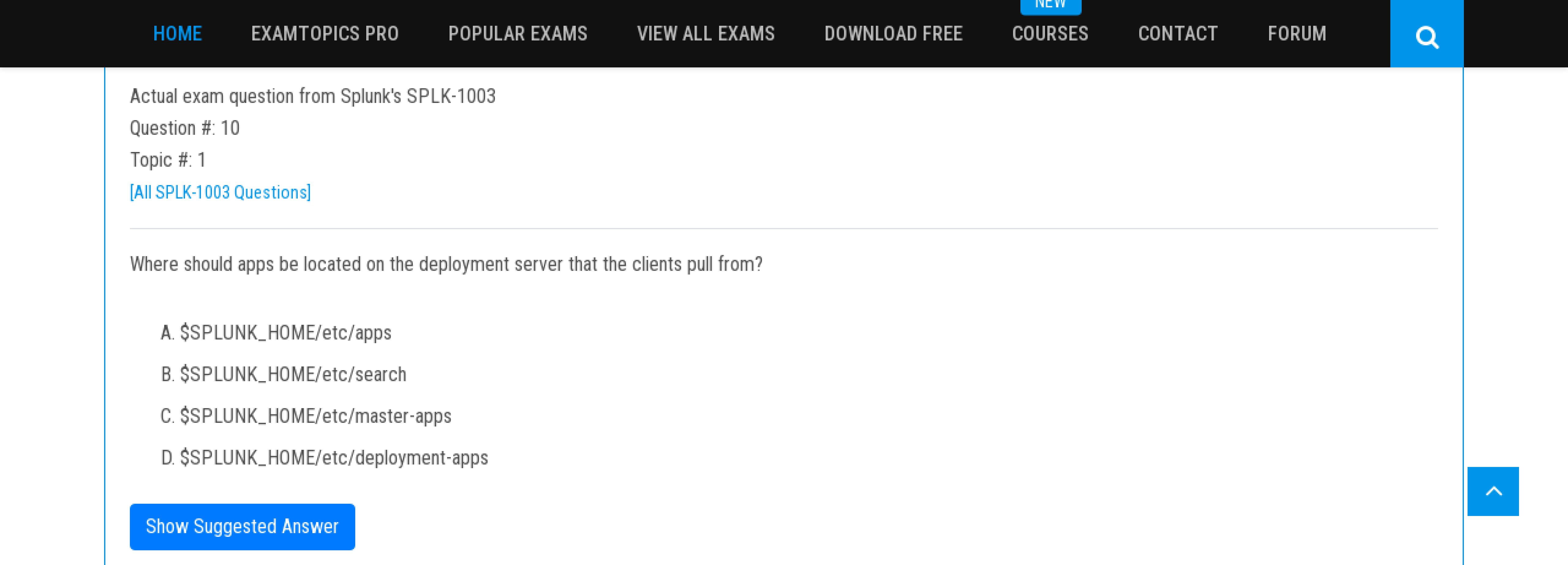
A. Deployer

B. Cluster master

C. Deployment server

D. Search head cluster master

Show Suggested Answer



Actual exam question from Splunk's SPLK-1003

Question #: 10

Topic #: 1

[All SPLK-1003 Questions]

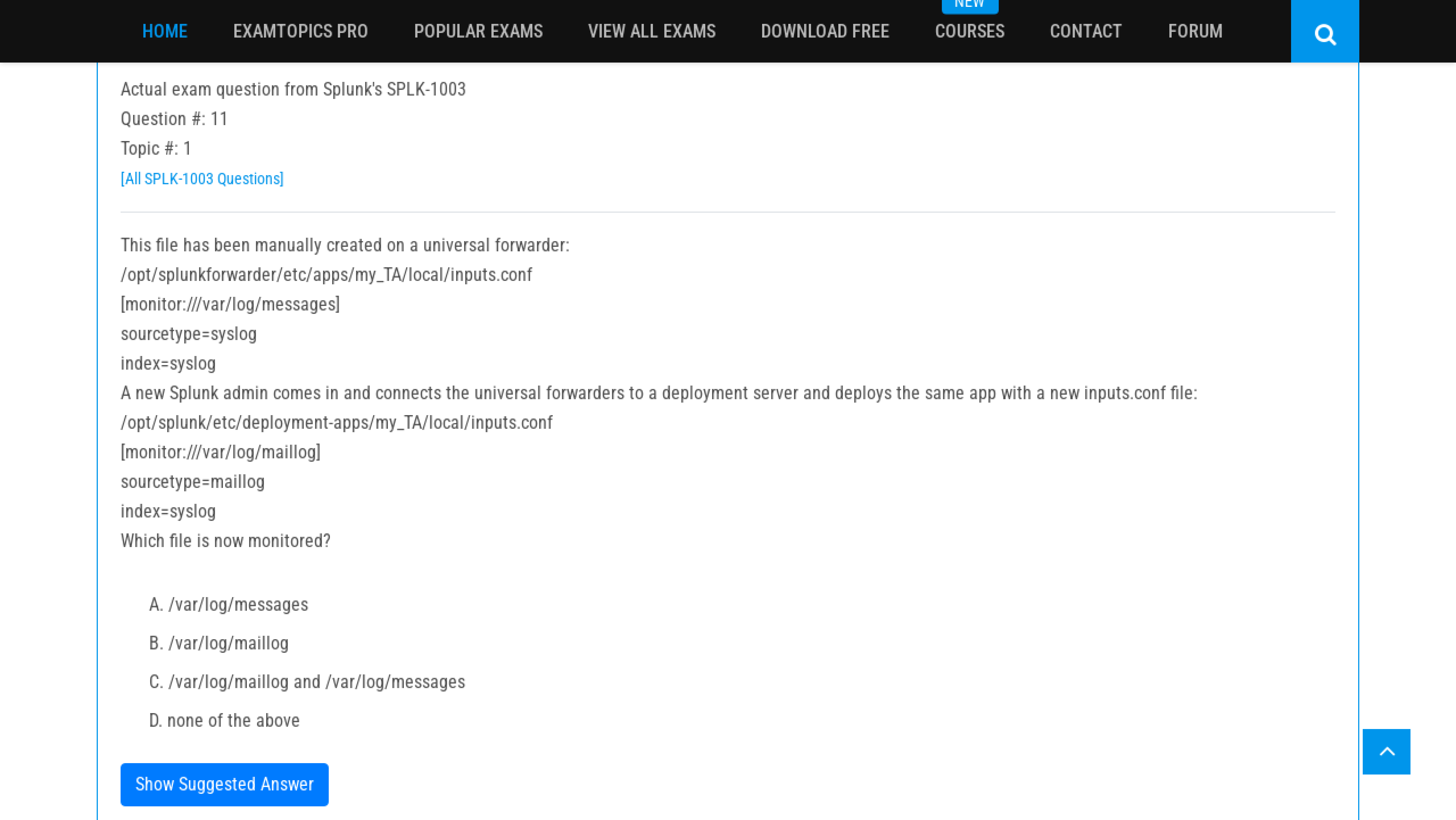
Where should apps be located on the deployment server that the clients pull from?

A. $SPLUNK_HOME/etc/apps

B. $SPLUNK_HOME/etc/search

C. $SPLUNK_HOME/etc/master-apps

D. $SPLUNK_HOME/etc/deployment-apps



Actual exam question from Splunk's SPLK-1003
Question #: 11
Topic #: 1
[All SPLK-1003 Questions]

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
```

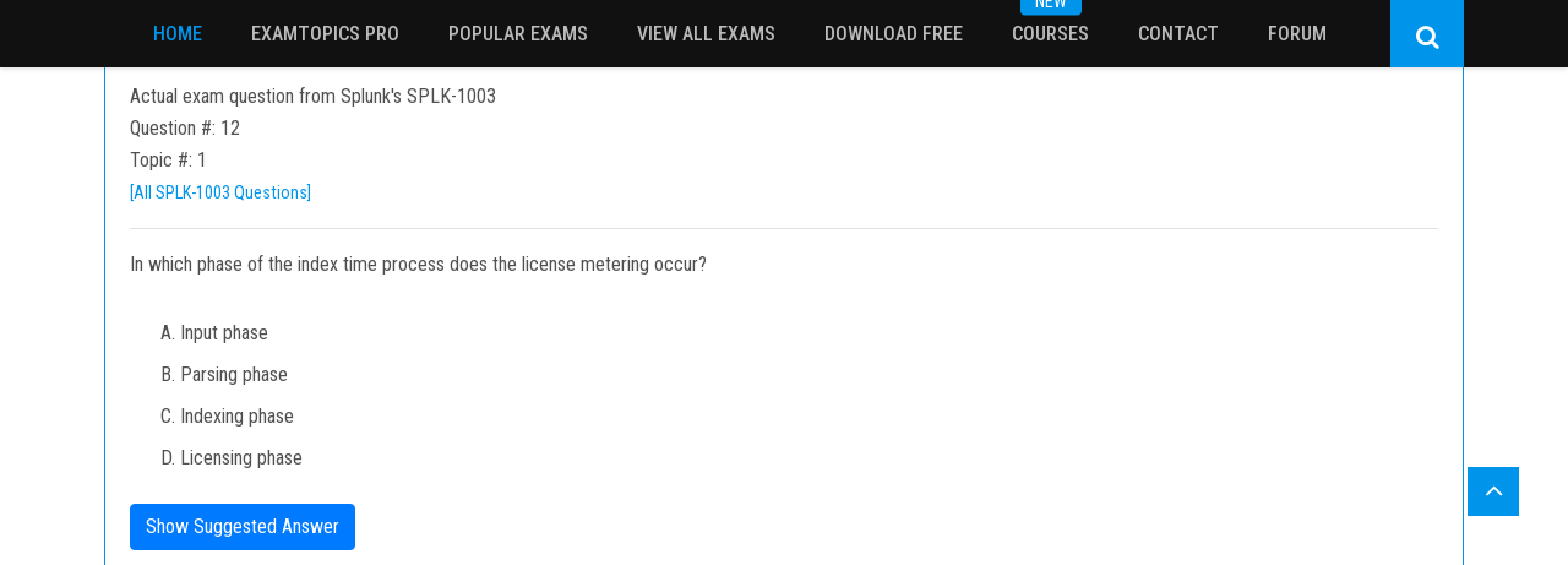
Which file is now monitored?

A. /var/log/messages

B. /var/log/maillog

C. /var/log/maillog and /var/log/messages

D. none of the above



Actual exam question from Splunk's SPLK-1003

Question #: 12

Topic #: 1

[All SPLK-1003 Questions]

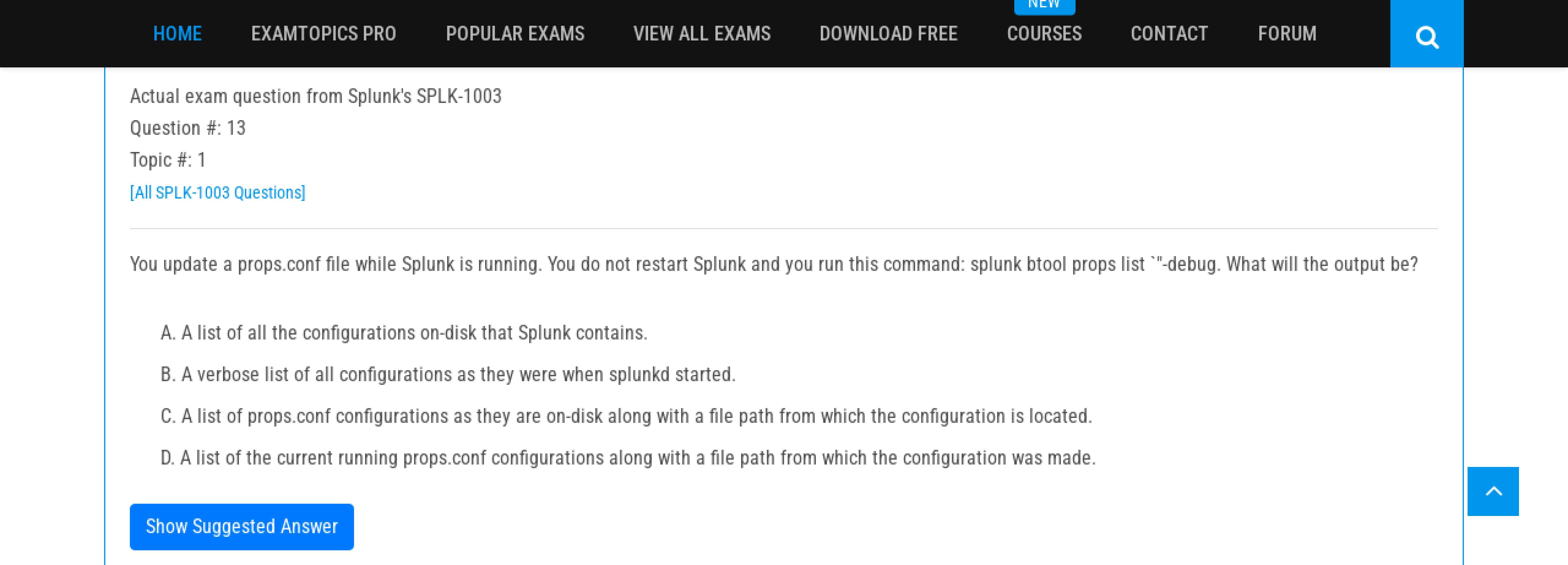
In which phase of the index time process does the license metering occur?

A. Input phase

B. Parsing phase

C. Indexing phase

D. Licensing phase



Actual exam question from Splunk's SPLK-1003

Question #: 13

Topic #: 1

[All SPLK-1003 Questions]

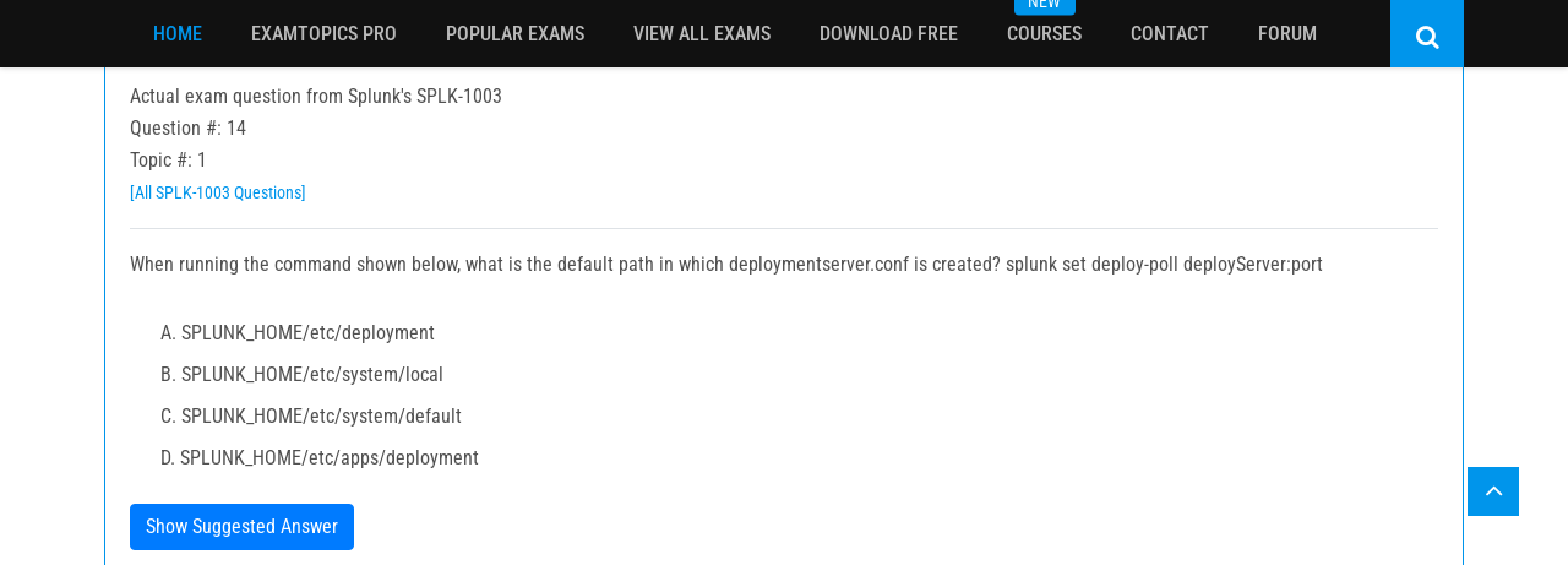
You update a props.conf file while Splunk is running. You do not restart Splunk and you run this command: splunk btool props list `"-debug. What will the output be?

A. A list of all the configurations on-disk that Splunk contains.

B. A verbose list of all configurations as they were when splunkd started.

C. A list of props.conf configurations as they are on-disk along with a file path from which the configuration is located.

D. A list of the current running props.conf configurations along with a file path from which the configuration was made.



Actual exam question from Splunk's SPLK-1003

Question #: 14

Topic #: 1

[All SPLK-1003 Questions]

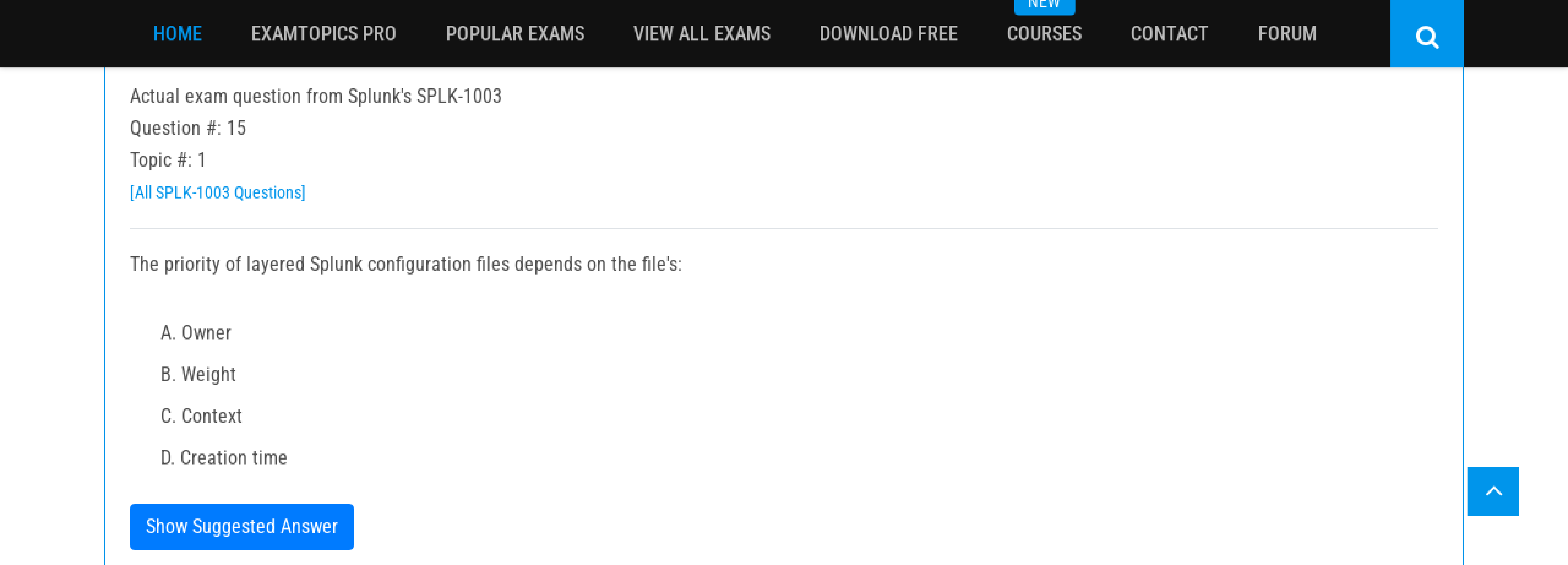
When running the command shown below, what is the default path in which deploymentserver.conf is created? splunk set deploy-poll deployServer:port

A. SPLUNK_HOME/etc/deployment

B. SPLUNK_HOME/etc/system/local

C. SPLUNK_HOME/etc/system/default

D. SPLUNK_HOME/etc/apps/deployment



Actual exam question from Splunk's SPLK-1003

Question #: 15

Topic #: 1

[All SPLK-1003 Questions]

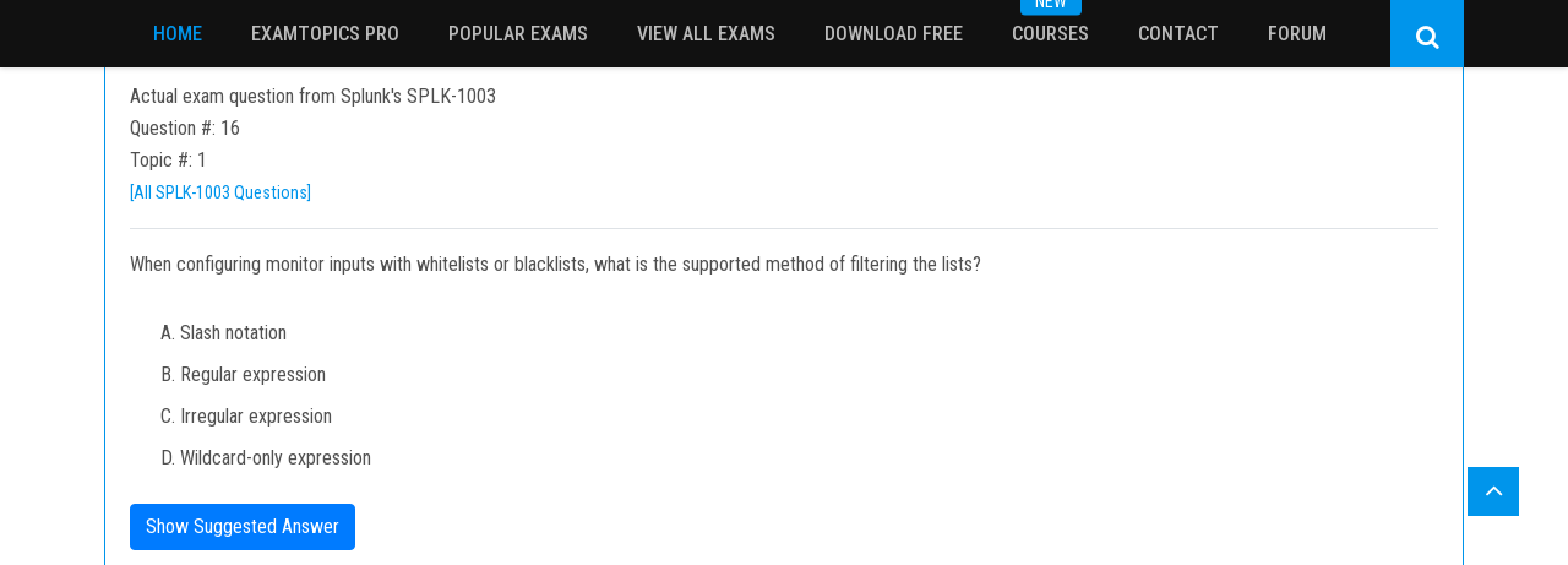
The priority of layered Splunk configuration files depends on the file's:

A. Owner

B. Weight

C. Context

D. Creation time



Actual exam question from Splunk's SPLK-1003

Question #: 16

Topic #: 1

[All SPLK-1003 Questions]

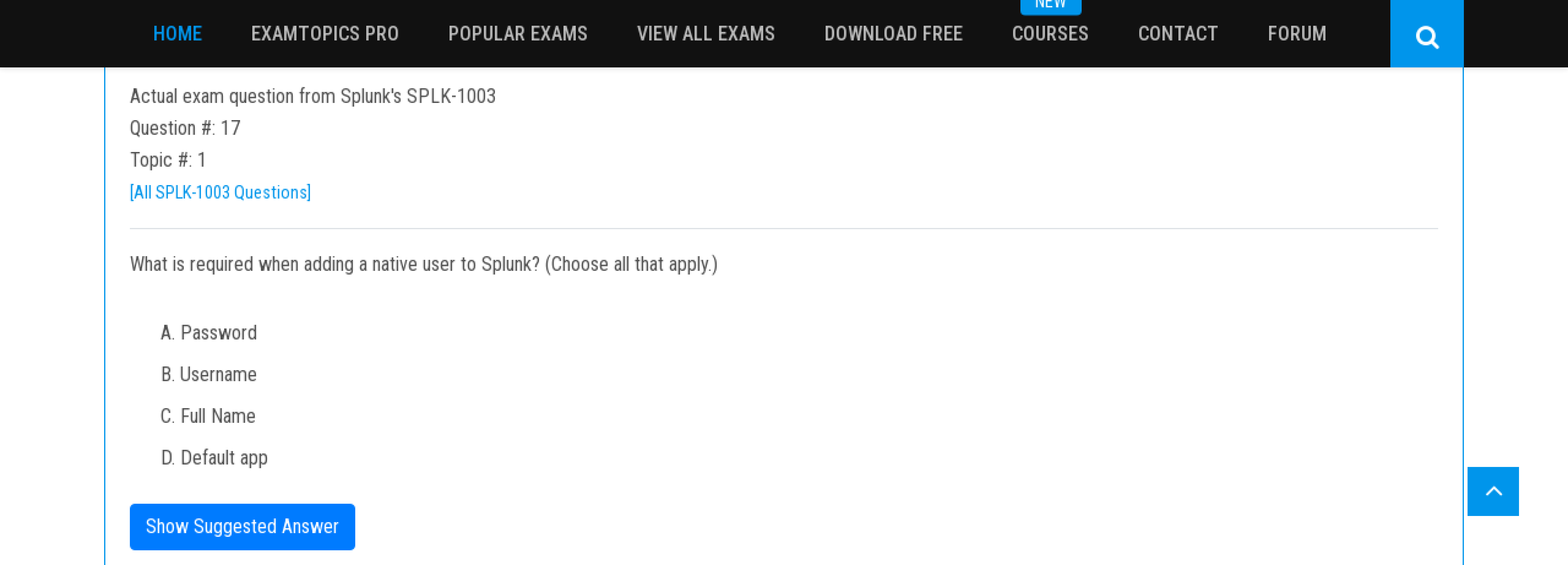
When configuring monitor inputs with whitelists or blacklists, what is the supported method of filtering the lists?

A. Slash notation

B. Regular expression

C. Irregular expression

D. Wildcard-only expression



Actual exam question from Splunk's SPLK-1003

Question #: 17

Topic #: 1

[All SPLK-1003 Questions]

What is required when adding a native user to Splunk? (Choose all that apply.)

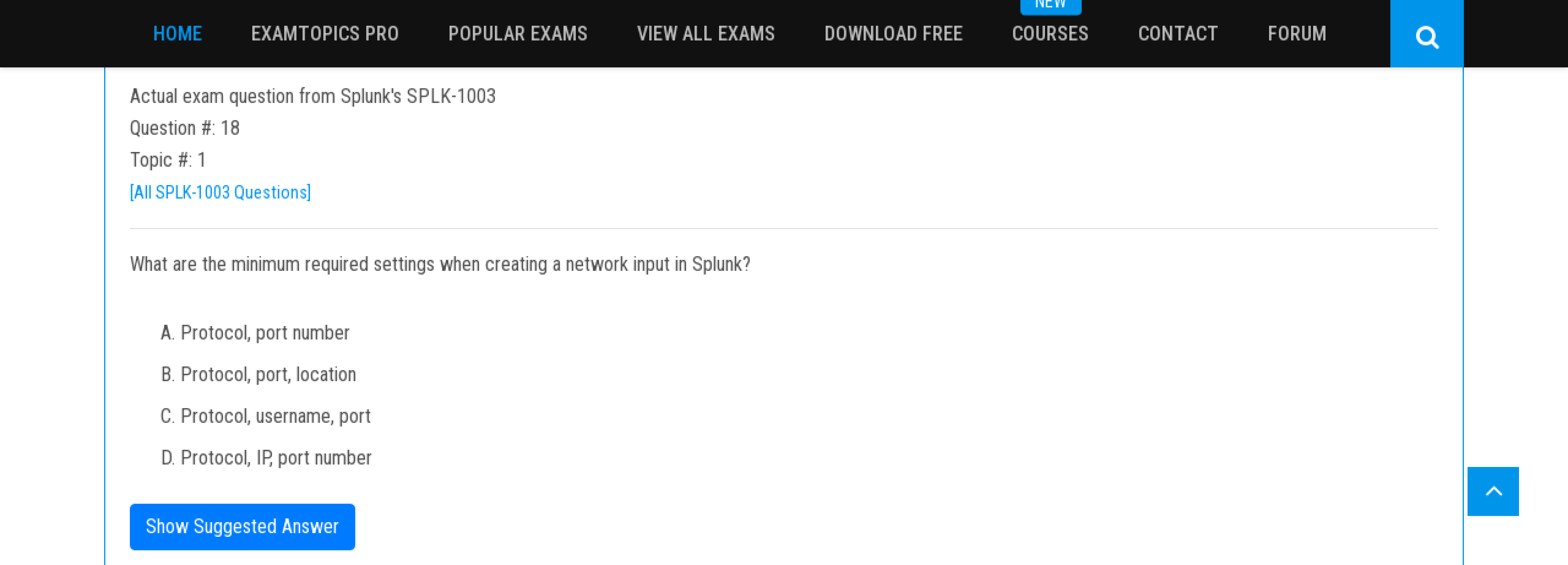
A. Password

B. Username

C. Full Name

D. Default app

Show Suggested Answer



Actual exam question from Splunk's SPLK-1003

Question #: 18

Topic #: 1

[All SPLK-1003 Questions]

What are the minimum required settings when creating a network input in Splunk?

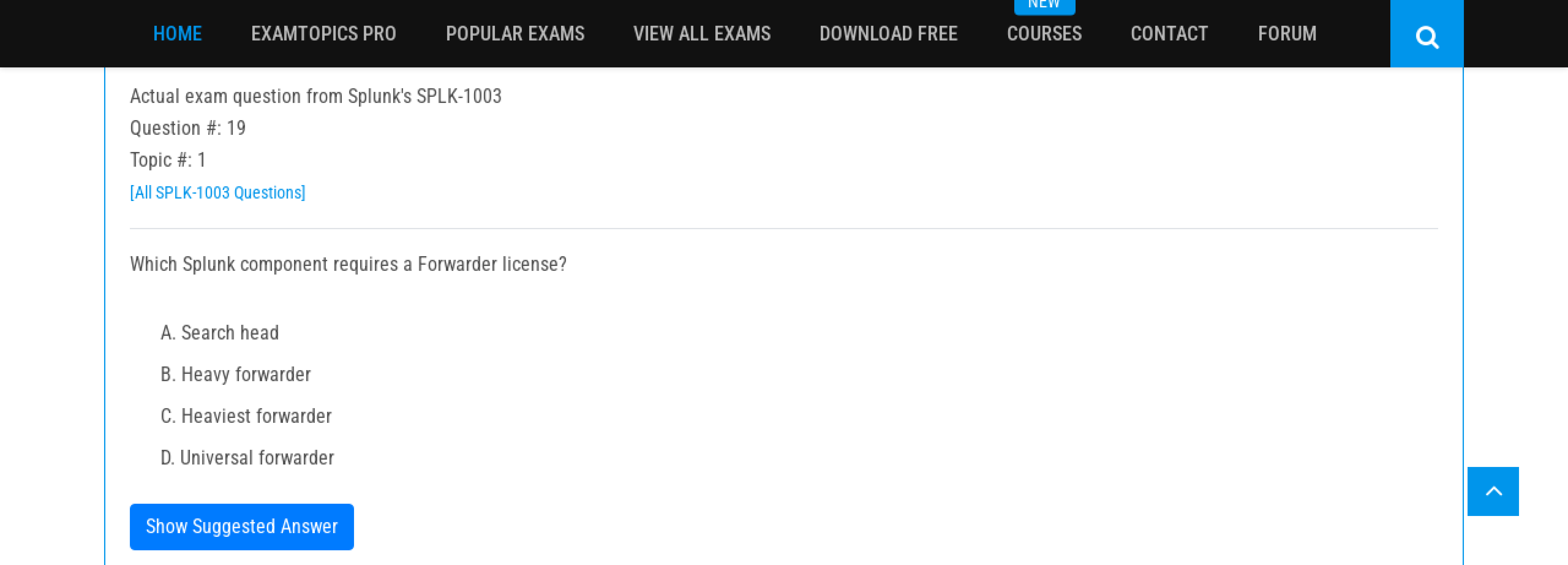
A. Protocol, port number

B. Protocol, port, location

C. Protocol, username, port

D. Protocol, IP, port number

Show Suggested Answer



Actual exam question from Splunk's SPLK-1003

Question #: 19

Topic #: 1

[All SPLK-1003 Questions]

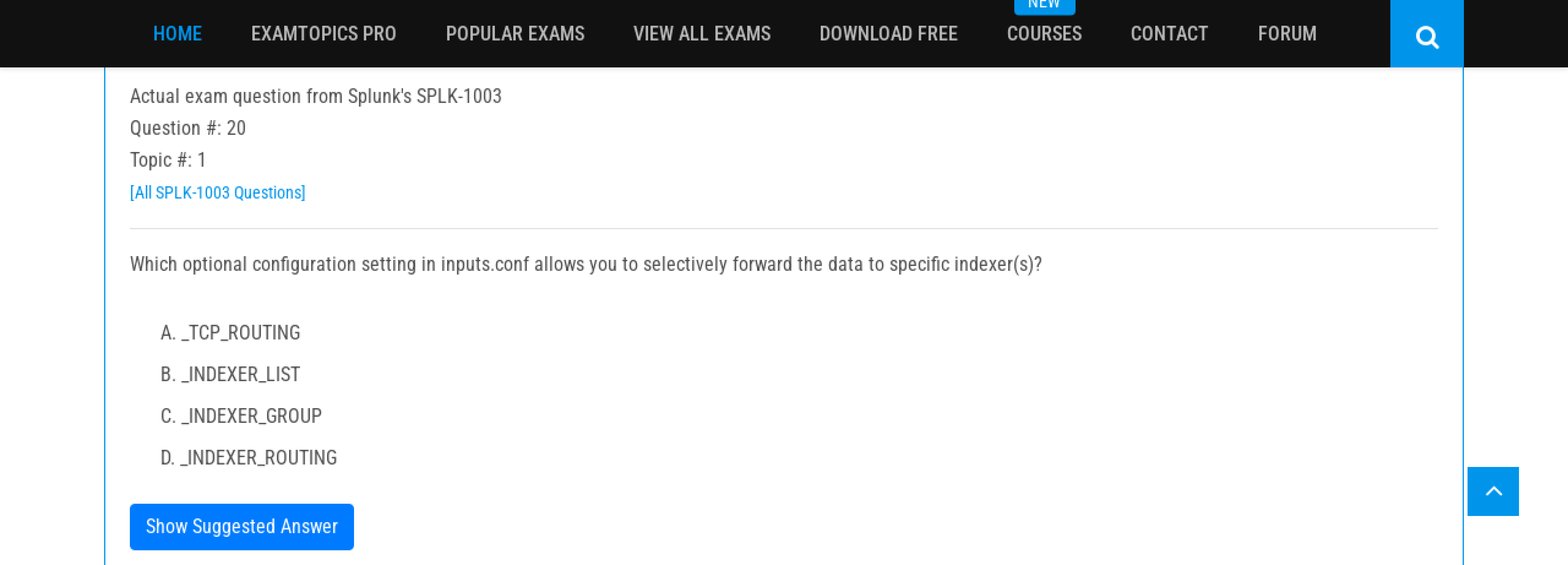
Which Splunk component requires a Forwarder license?

A. Search head

B. Heavy forwarder

C. Heaviest forwarder

D. Universal forwarder



Actual exam question from Splunk's SPLK-1003

Question #: 20

Topic #: 1

[All SPLK-1003 Questions]

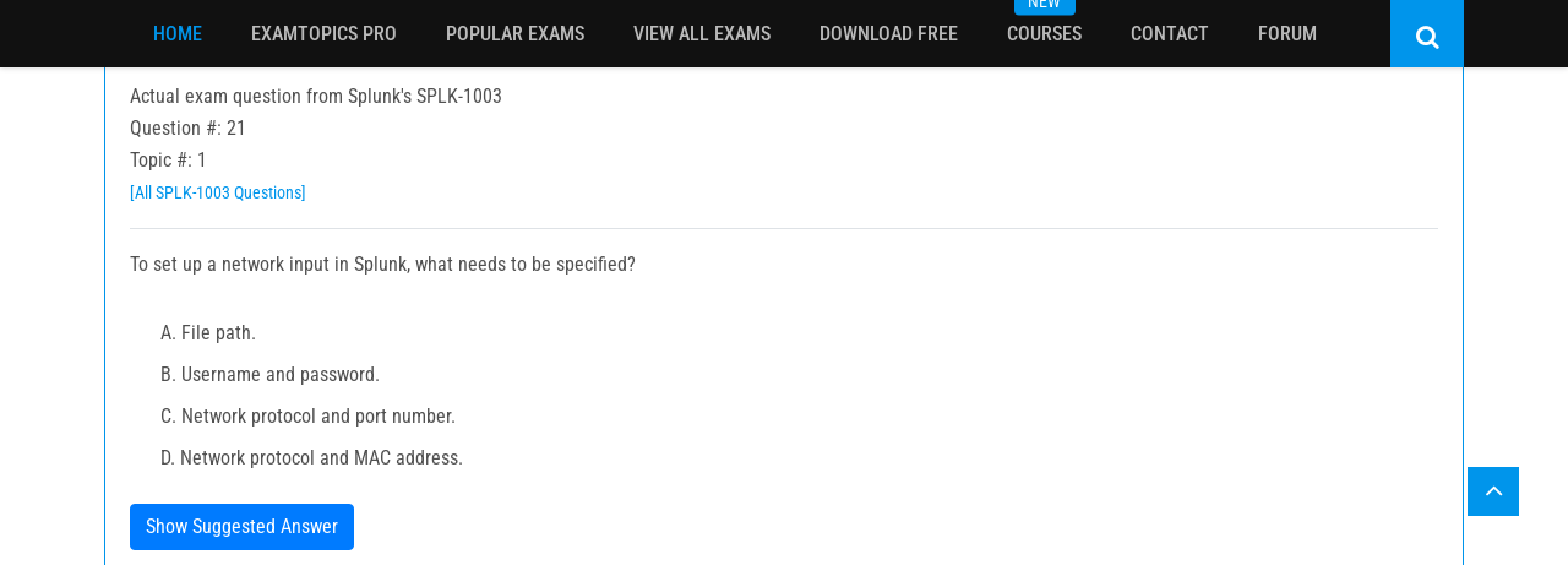
Which optional configuration setting in inputs.conf allows you to selectively forward the data to specific indexer(s)?

A. _TCP_ROUTING

B. _INDEXER_LIST

C. _INDEXER_GROUP

D. _INDEXER_ROUTING



Actual exam question from Splunk's SPLK-1003

Question #: 21

Topic #: 1

[All SPLK-1003 Questions]

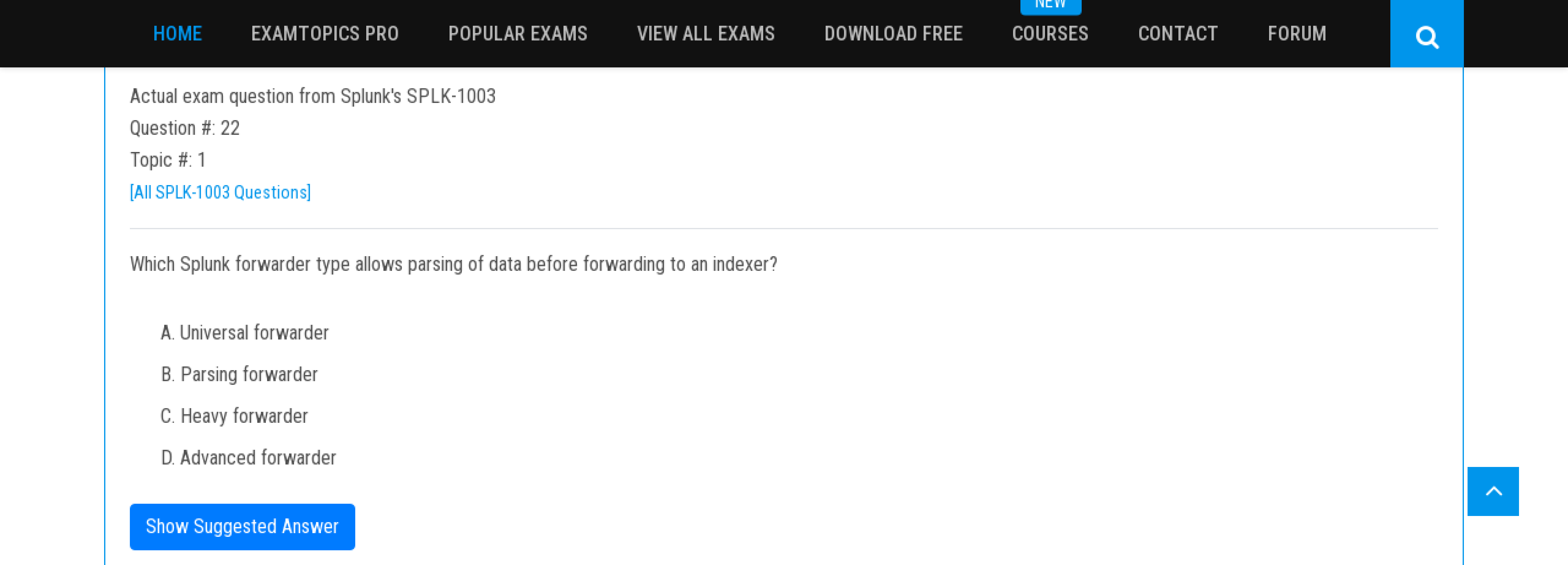
To set up a network input in Splunk, what needs to be specified?

A. File path.

B. Username and password.

C. Network protocol and port number.

D. Network protocol and MAC address.



Actual exam question from Splunk's SPLK-1003

Question #: 22

Topic #: 1

[All SPLK-1003 Questions]

Which Splunk forwarder type allows parsing of data before forwarding to an indexer?

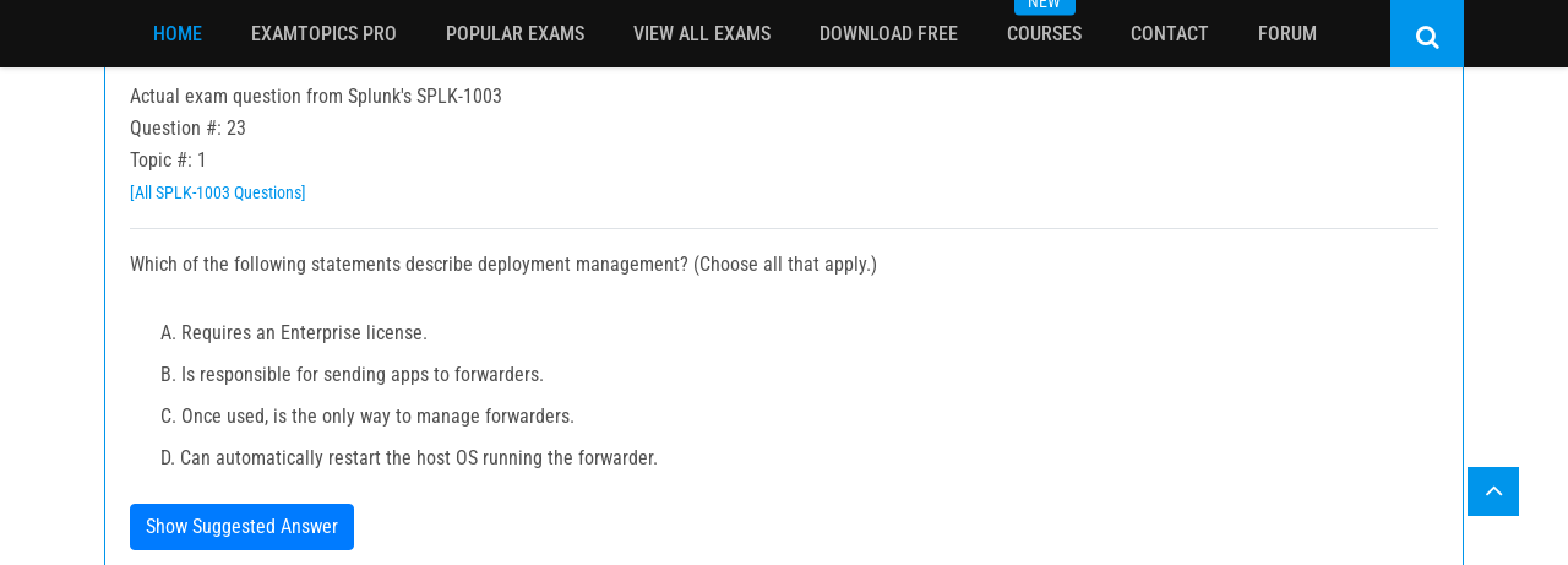
A. Universal forwarder

B. Parsing forwarder

C. Heavy forwarder

D. Advanced forwarder

Show Suggested Answer



Actual exam question from Splunk's SPLK-1003

Question #: 23

Topic #: 1

[All SPLK-1003 Questions]

Which of the following statements describe deployment management? (Choose all that apply.)

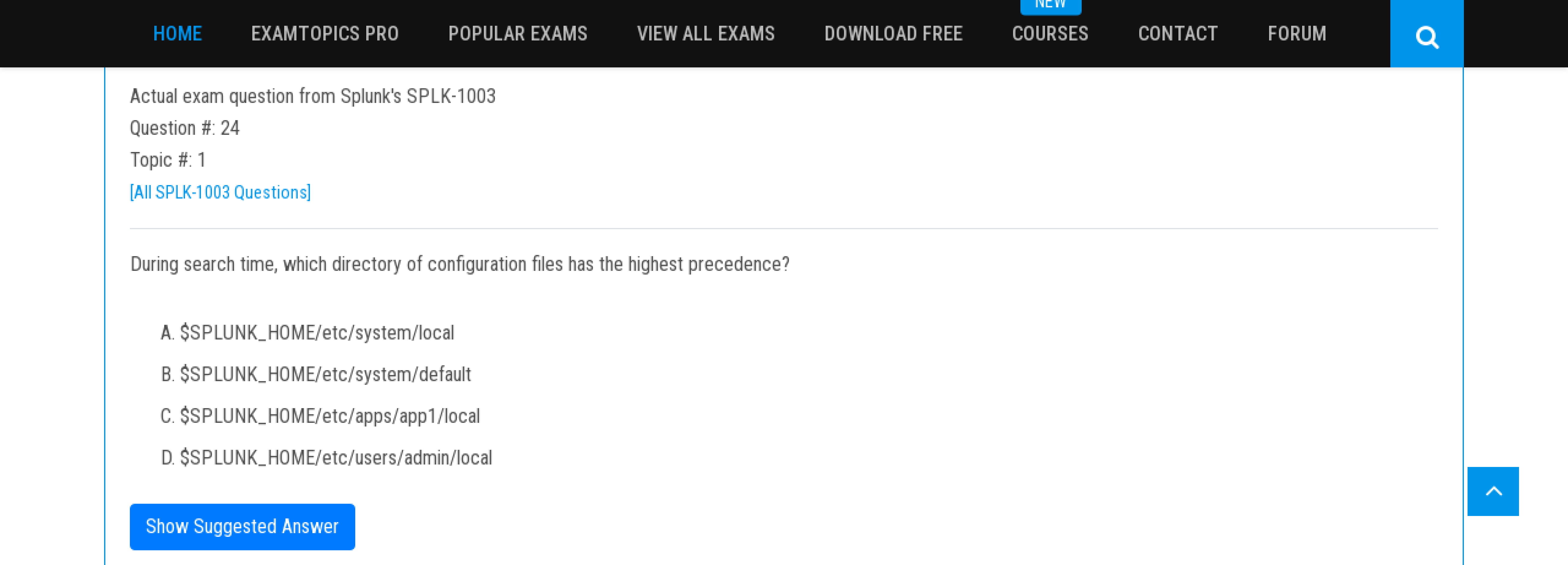
A. Requires an Enterprise license.

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.

Show Suggested Answer



Actual exam question from Splunk's SPLK-1003

Question #: 24

Topic #: 1

[All SPLK-1003 Questions]

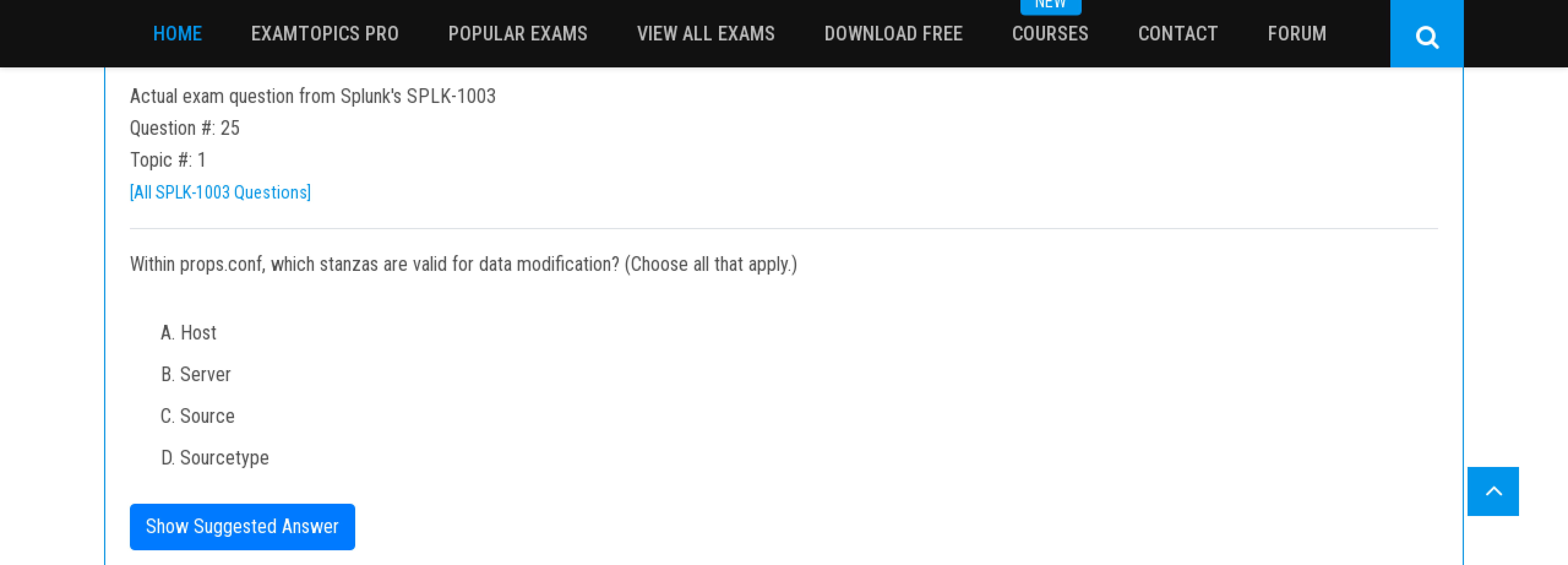
During search time, which directory of configuration files has the highest precedence?

A. $SPLUNK_HOME/etc/system/local

B. $SPLUNK_HOME/etc/system/default

C. $SPLUNK_HOME/etc/apps/app1/local

D. $SPLUNK_HOME/etc/users/admin/local



Actual exam question from Splunk's SPLK-1003

Question #: 25

Topic #: 1

[All SPLK-1003 Questions]

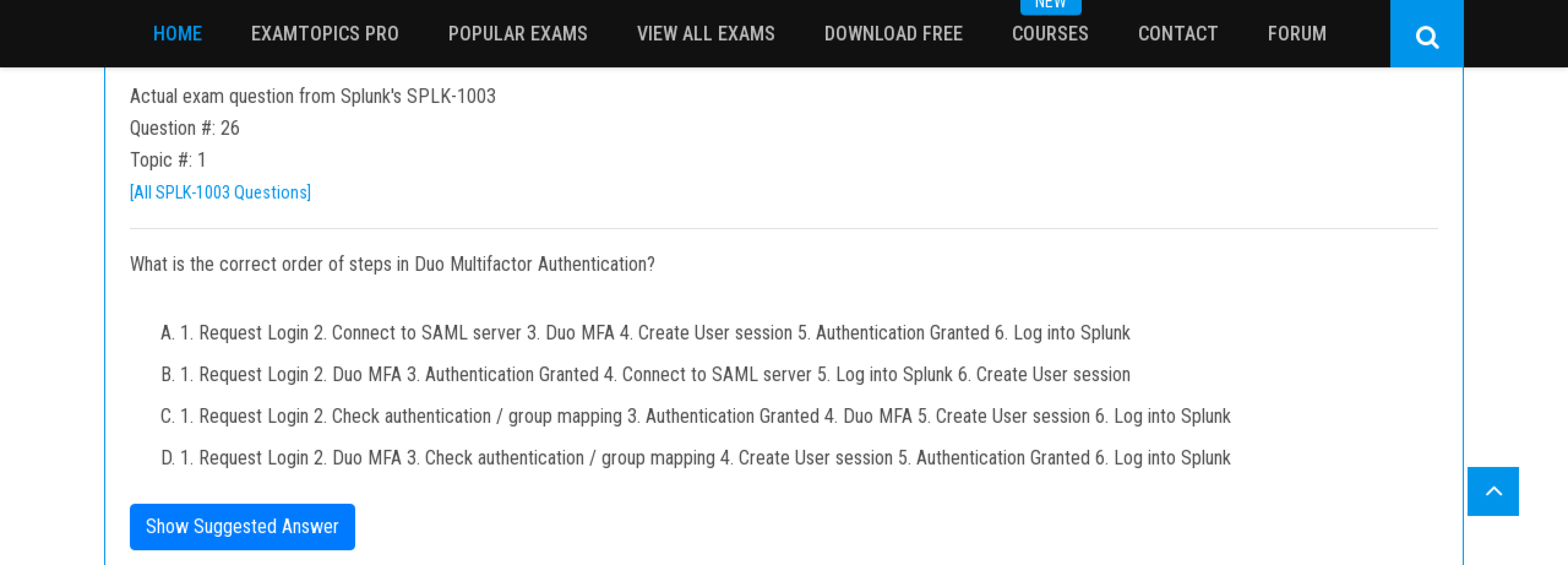
Within props.conf, which stanzas are valid for data modification? (Choose all that apply.)

A. Host

B. Server

C. Source

D. Sourcetype



Actual exam question from Splunk's SPLK-1003

Question #: 26

Topic #: 1

[All SPLK-1003 Questions]

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

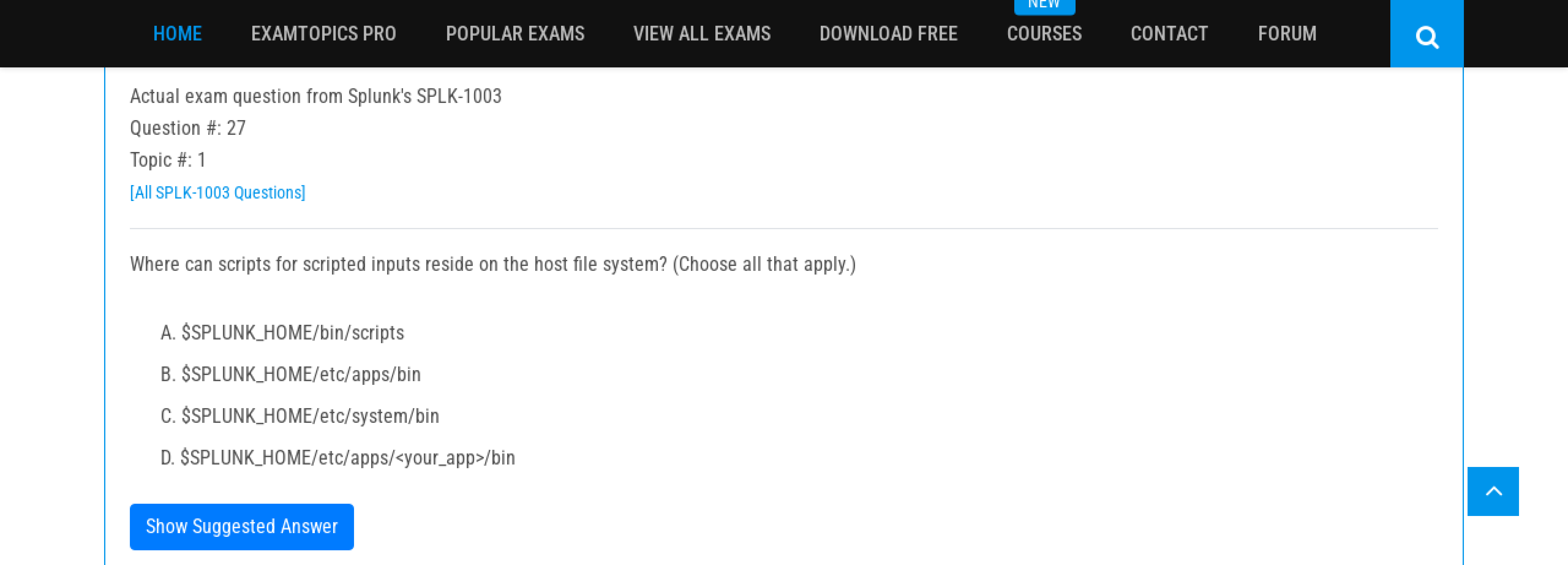
A. 1. Request Login 2. Connect to SAML server 3. Duo MFA 4. Create User session 5. Authentication Granted 6. Log into Splunk

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

Show Suggested Answer



Actual exam question from Splunk's SPLK-1003

Question #: 27

Topic #: 1

[All SPLK-1003 Questions]

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

A. $SPLUNK_HOME/bin/scripts

B. $SPLUNK_HOME/etc/apps/bin

C. $SPLUNK_HOME/etc/system/bin

D. $SPLUNK_HOME/etc/apps/<your_app>/bin

Actual exam question from Splunk's SPLK-1003

Question #: 28

Topic #: 1

[All SPLK-1003 Questions]

How does the Monitoring Console monitor forwarders?

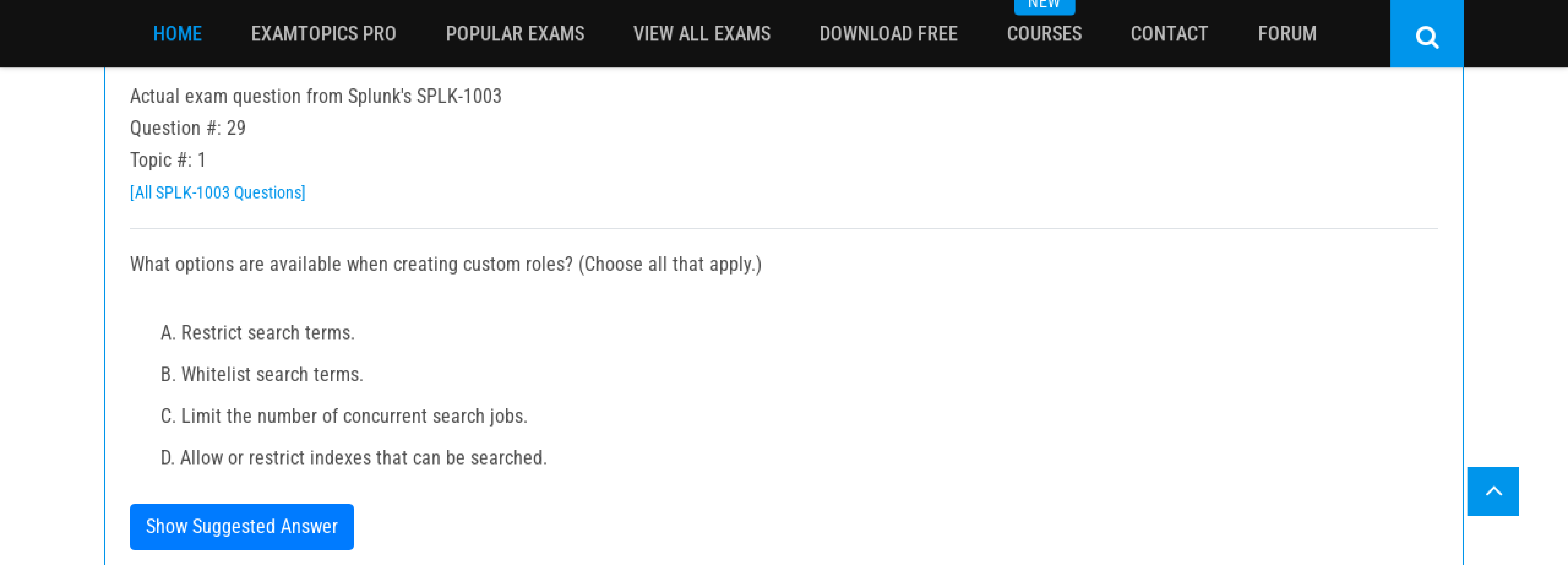
A. By pulling internal logs from forwarders.

B. By using the forwarder monitoring add-on.

C. With internal logs forwarded by forwarders.

D. With internal logs forwarded by deployment server.

Show Suggested Answer



Actual exam question from Splunk's SPLK-1003

Question #: 29

Topic #: 1

[All SPLK-1003 Questions]

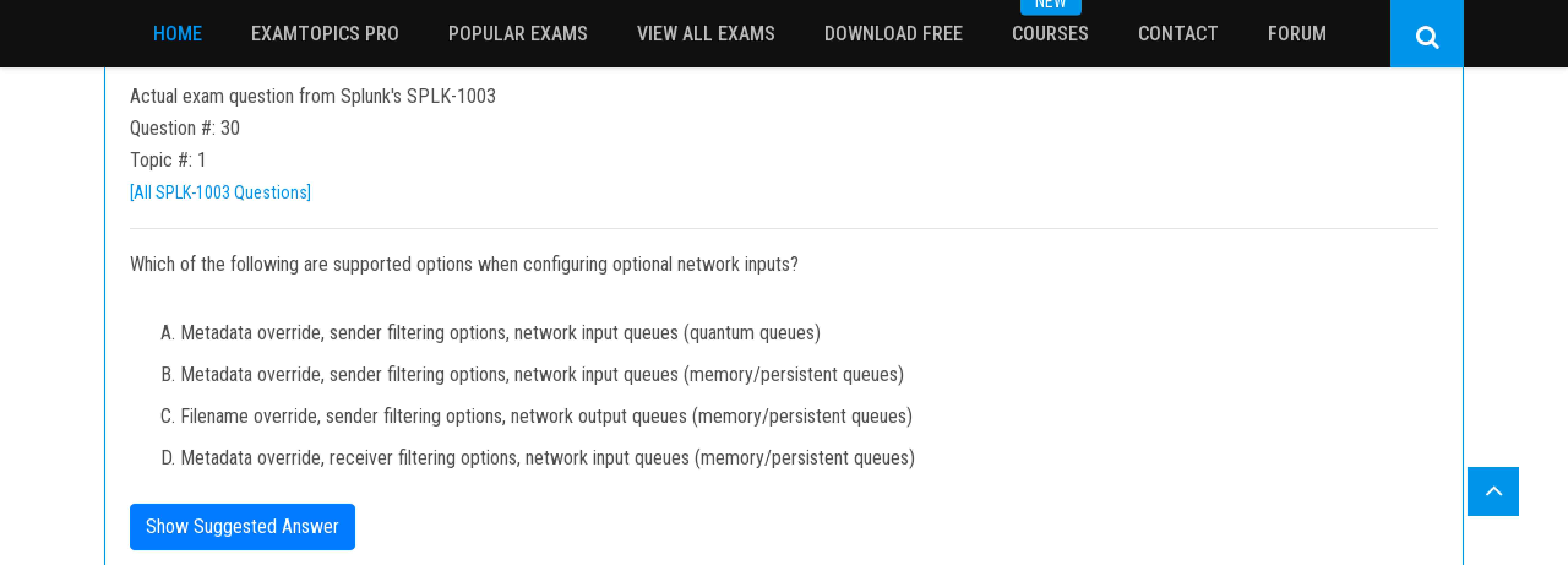
What options are available when creating custom roles? (Choose all that apply.)

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.



Actual exam question from Splunk's SPLK-1003

Question #: 30

Topic #: 1

[All SPLK-1003 Questions]

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

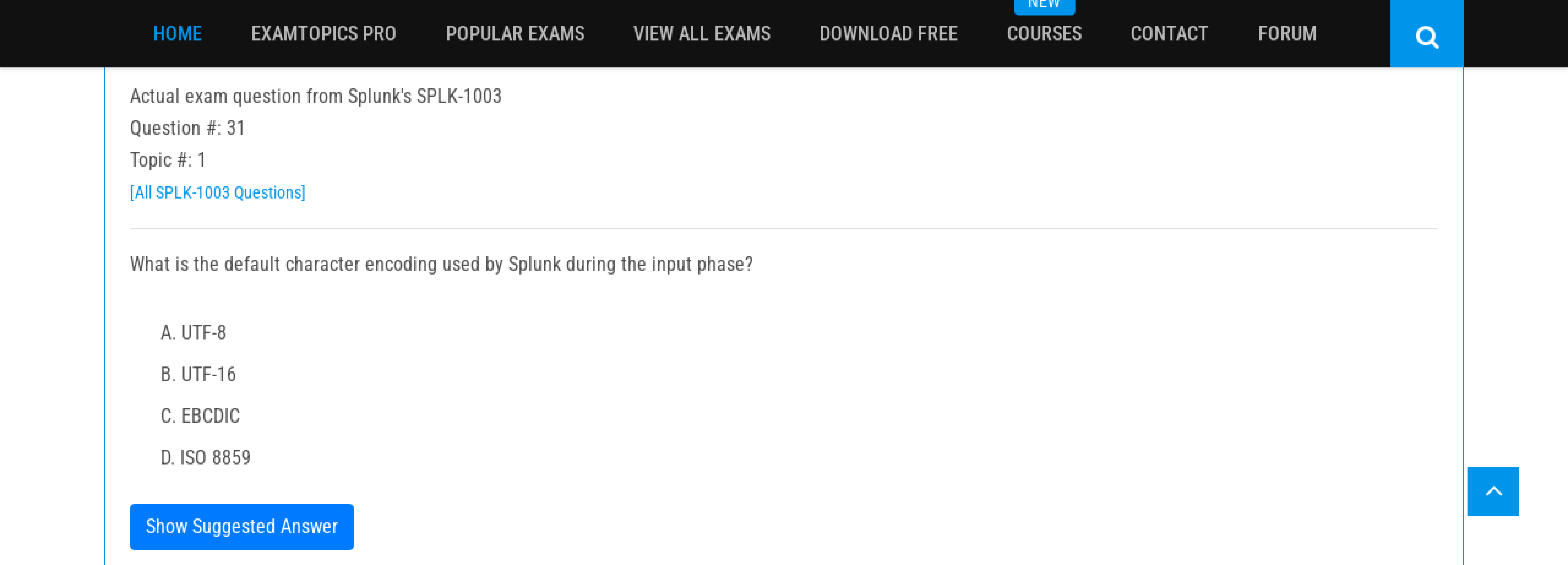
A. Metadata override, sender filtering options, network input queues (quantum queues)

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)

Show Suggested Answer



Actual exam question from Splunk's SPLK-1003

Question #: 31

Topic #: 1

[All SPLK-1003 Questions]

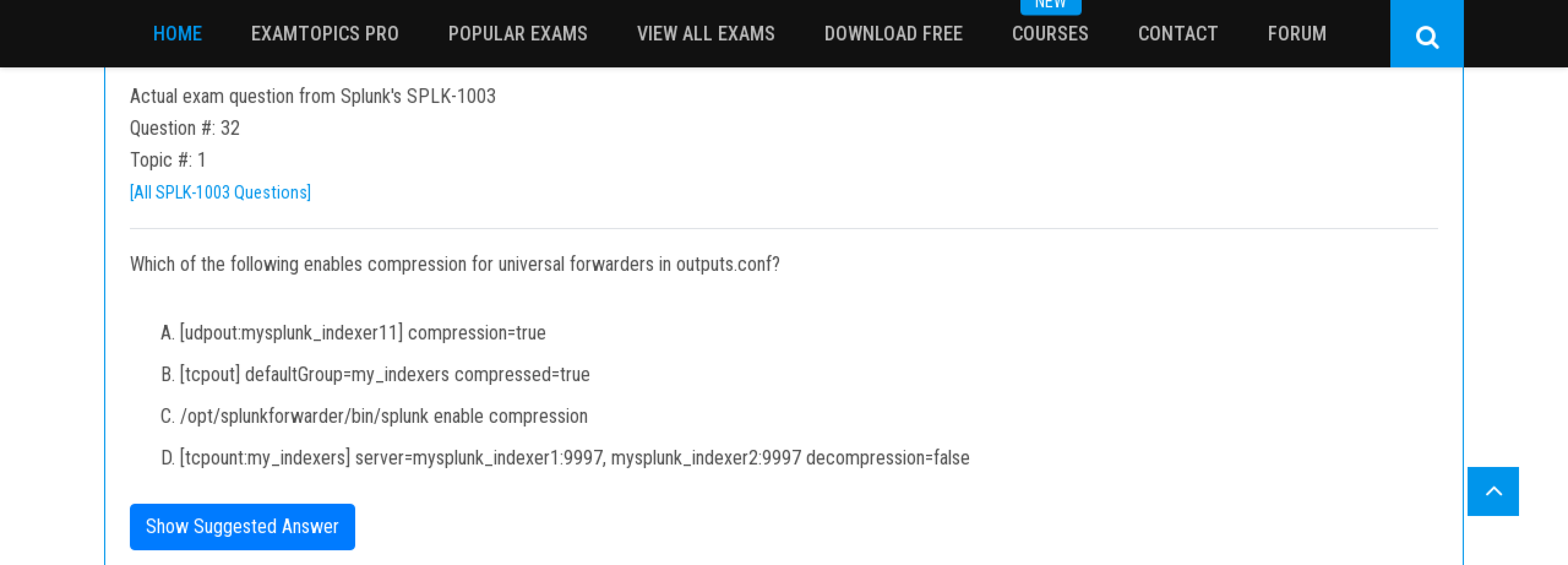
What is the default character encoding used by Splunk during the input phase?

A. UTF-8

B. UTF-16

C. EBCDIC

D. ISO 8859



Actual exam question from Splunk's SPLK-1003

Question #: 32

Topic #: 1

[All SPLK-1003 Questions]

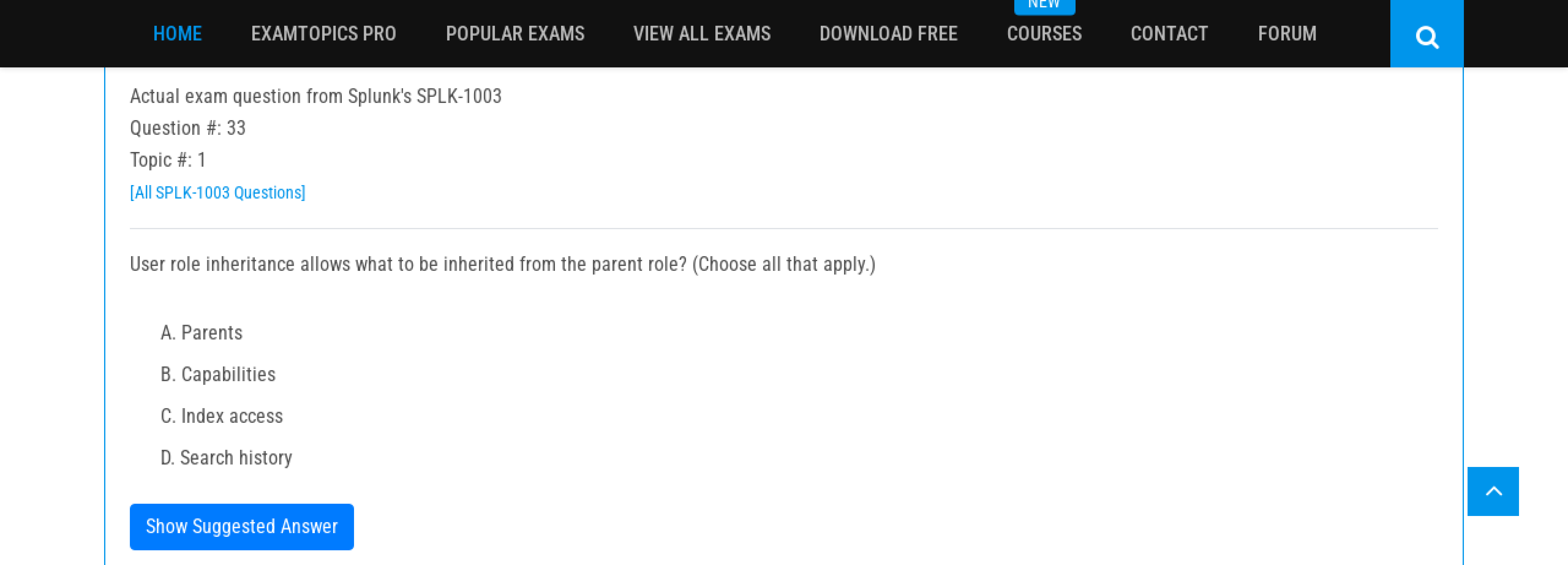
Which of the following enables compression for universal forwarders in outputs.conf?

A. [udpout:mysplunk_indexer11] compression=true

B. [tcpout] defaultGroup=my_indexers compressed=true

C. /opt/splunkforwarder/bin/splunk enable compression

D. [tcpount:my_indexers] server=mysplunk_indexer1:9997, mysplunk_indexer2:9997 decompression=false



Actual exam question from Splunk's SPLK-1003

Question #: 33

Topic #: 1

[All SPLK-1003 Questions]

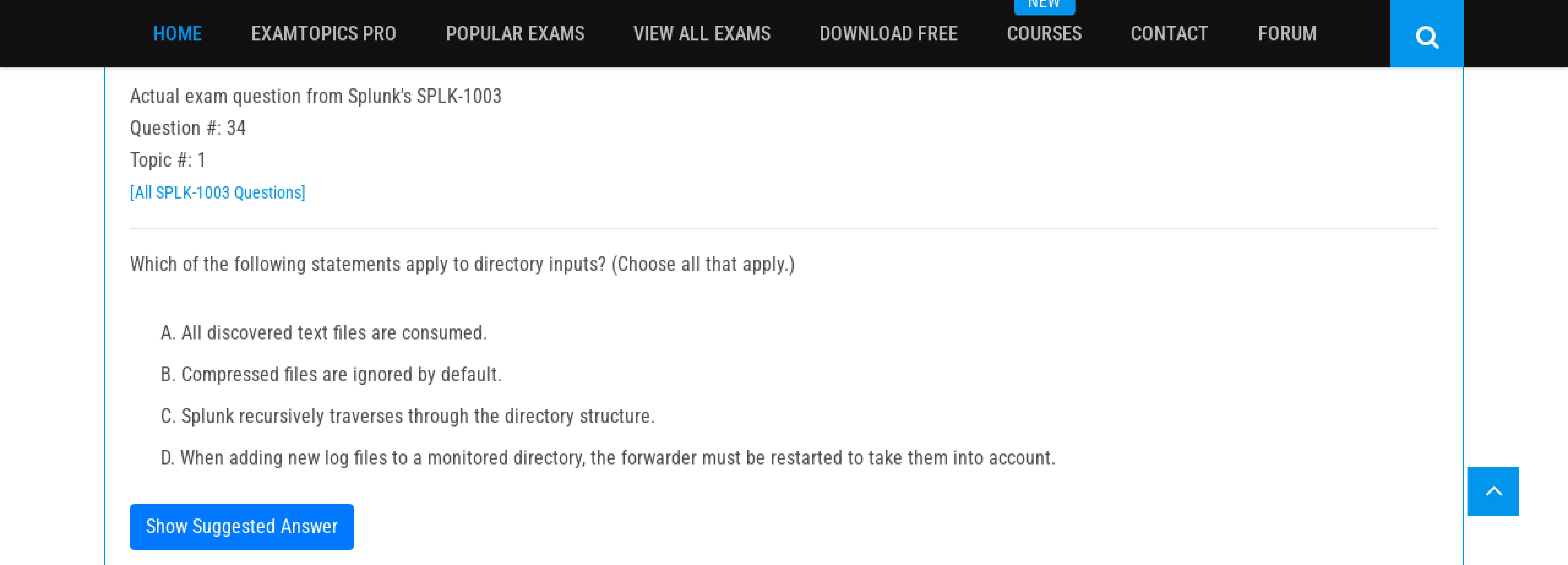
User role inheritance allows what to be inherited from the parent role? (Choose all that apply.)

A. Parents

B. Capabilities

C. Index access

D. Search history



Actual exam question from Splunk's SPLK-1003

Question #: 34

Topic #: 1

[All SPLK-1003 Questions]

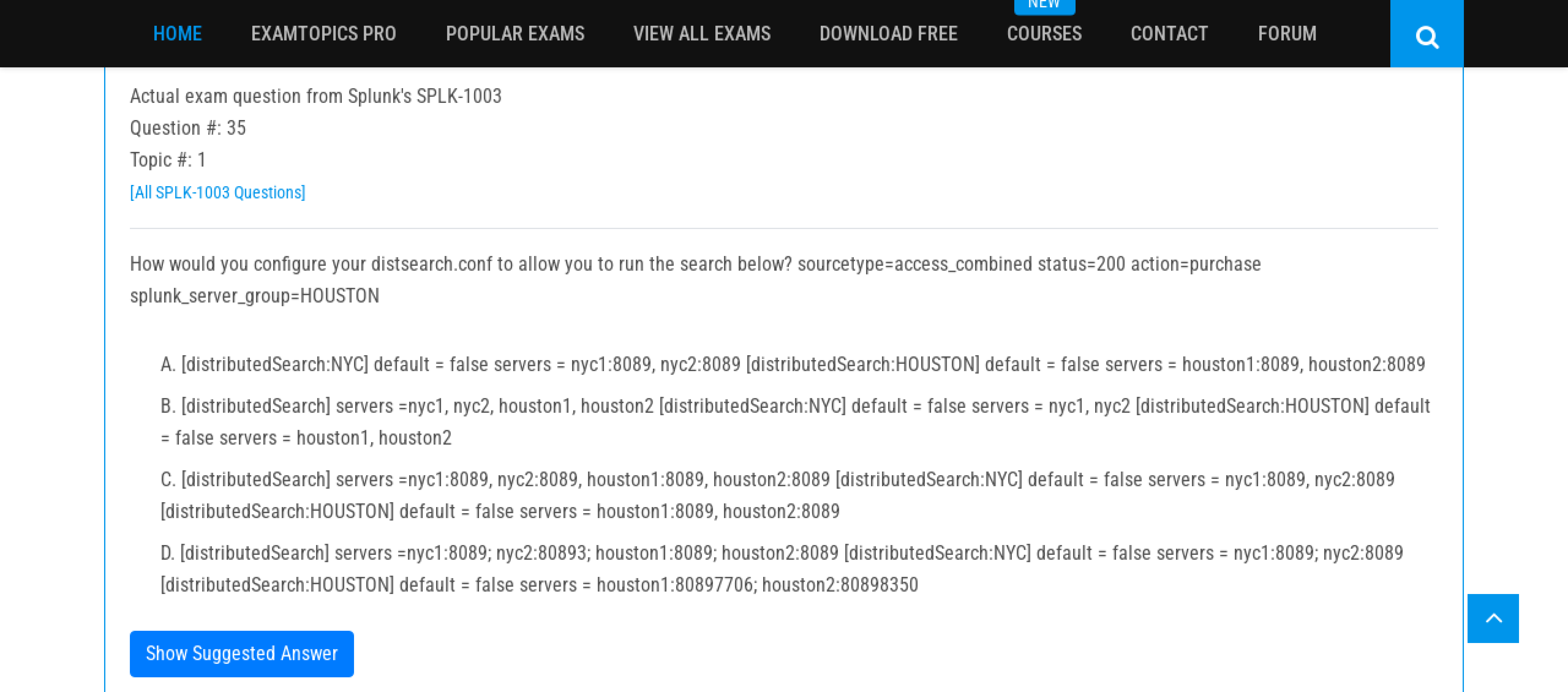
Which of the following statements apply to directory inputs? (Choose all that apply.)

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.



Actual exam question from Splunk's SPLK-1003

Question #: 35

Topic #: 1

[All SPLK-1003 Questions]

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

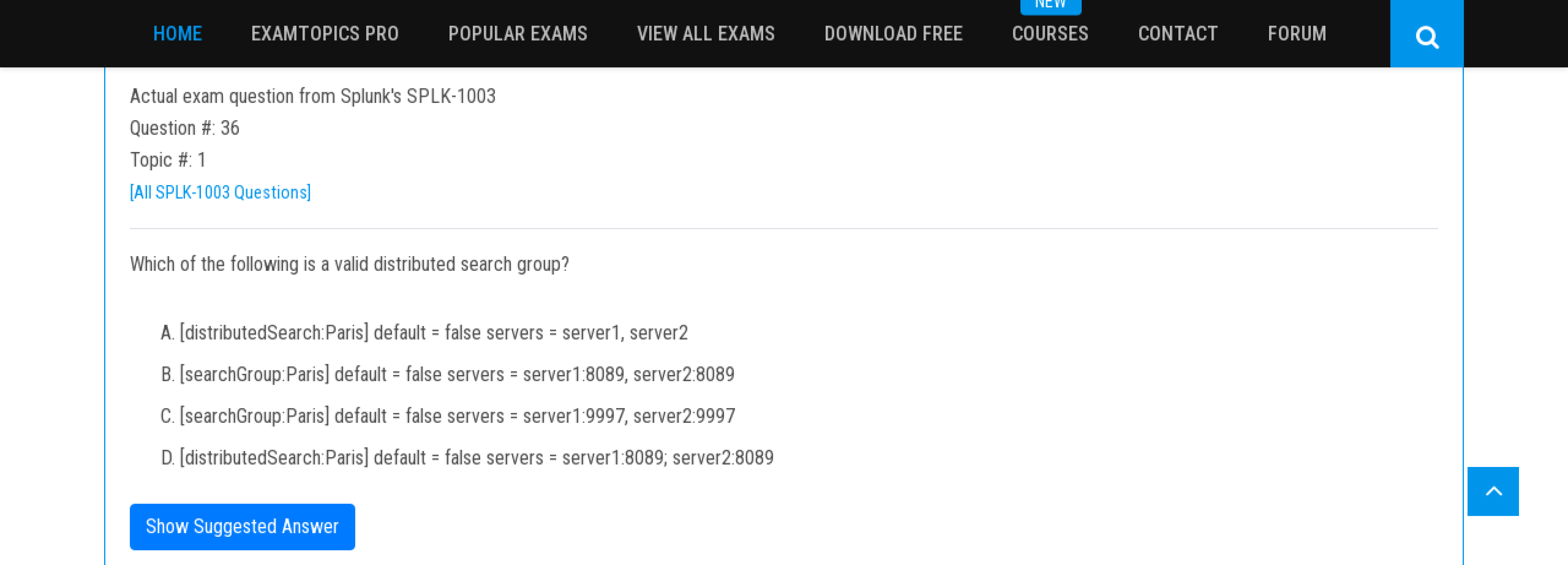
A. [distributedSearch:NYC] default = false servers = nyc1:8089, nyc2:8089 [distributedSearch:HOUSTON] default = false servers = houston1:8089, houston2:8089

B. [distributedSearch] servers =nyc1, nyc2, houston1, houston2 [distributedSearch:NYC] default = false servers = nyc1, nyc2 [distributedSearch:HOUSTON] default = false servers = houston1, houston2

C. [distributedSearch] servers =nyc1:8089, nyc2:8089, houston1:8089, houston2:8089 [distributedSearch:NYC] default = false servers = nyc1:8089, nyc2:8089 [distributedSearch:HOUSTON] default = false servers = houston1:8089, houston2:8089

D. [distributedSearch] servers =nyc1:8089; nyc2:80893; houston1:8089; houston2:8089 [distributedSearch:NYC] default = false servers = nyc1:8089; nyc2:8089 [distributedSearch:HOUSTON] default = false servers = houston1:80897706; houston2:80898350

Show Suggested Answer



Actual exam question from Splunk's SPLK-1003

Question #: 36

Topic #: 1

[All SPLK-1003 Questions]

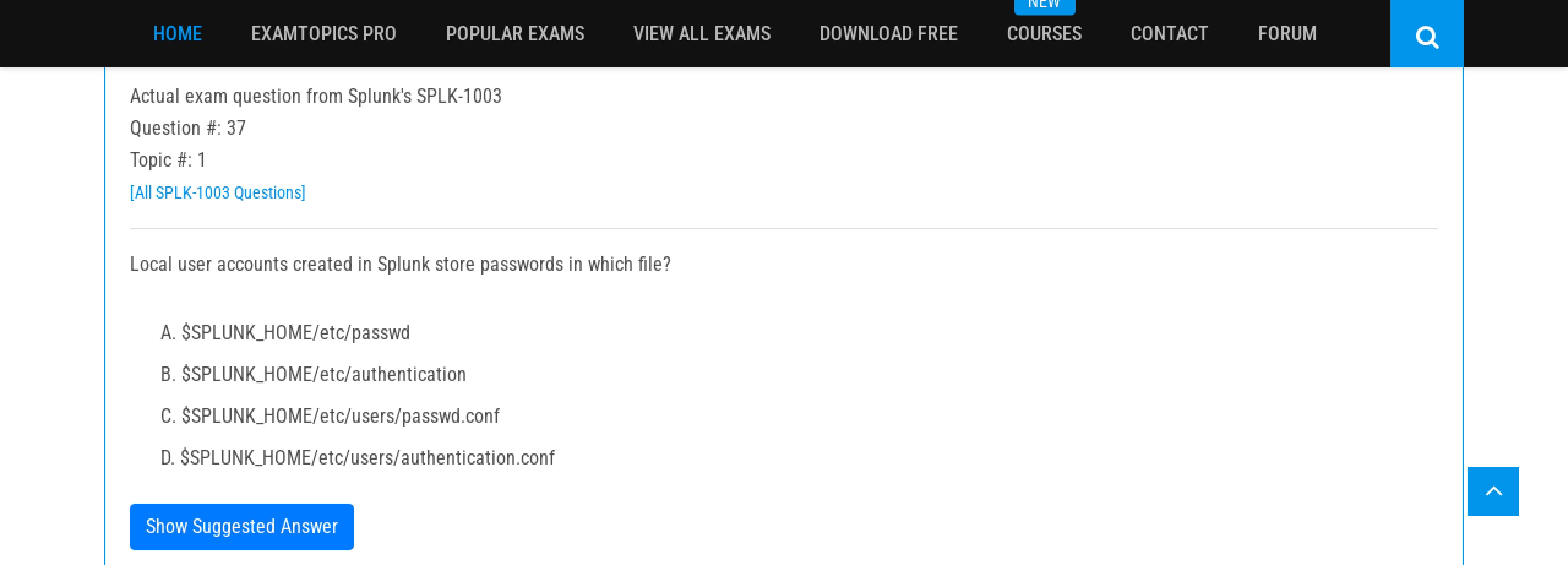
Which of the following is a valid distributed search group?

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



Actual exam question from Splunk's SPLK-1003

Question #: 37

Topic #: 1

[All SPLK-1003 Questions]

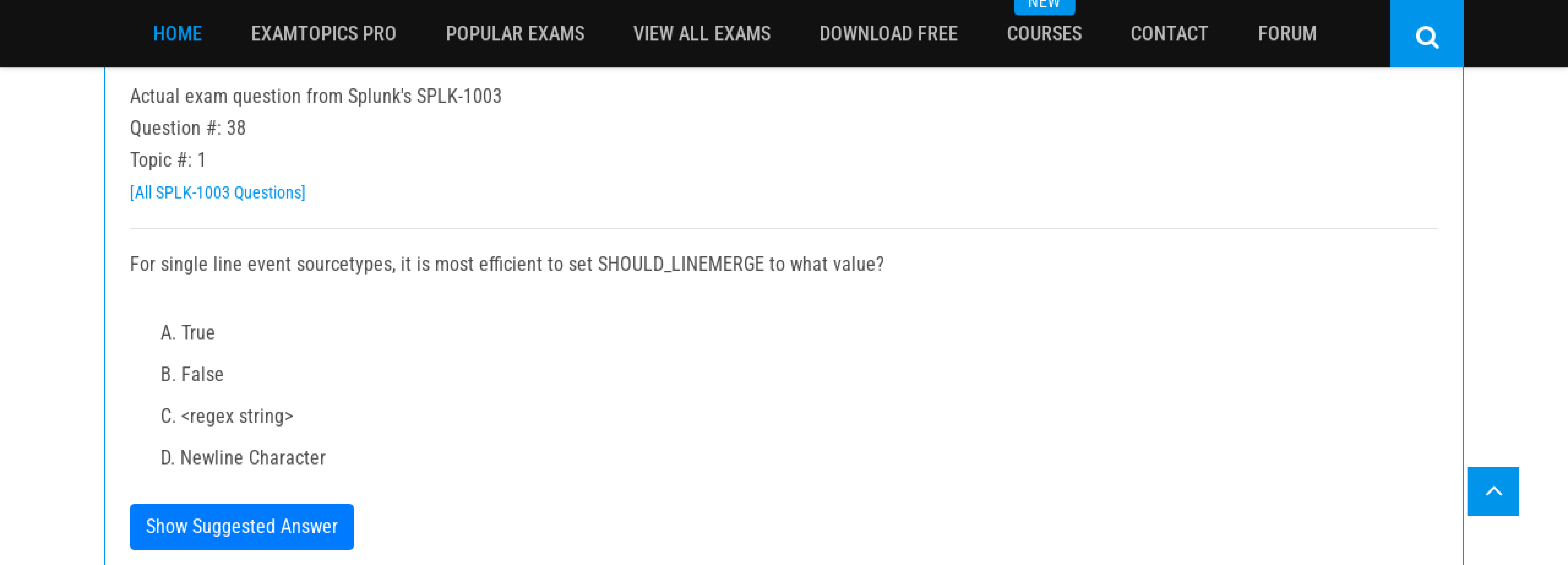
Local user accounts created in Splunk store passwords in which file?

A. $SPLUNK_HOME/etc/passwd

B. $SPLUNK_HOME/etc/authentication

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

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



Actual exam question from Splunk's SPLK-1003

Question #: 38

Topic #: 1

[All SPLK-1003 Questions]

For single line event sourcetypes, it is most efficient to set SHOULD_LINEMERGE to what value?

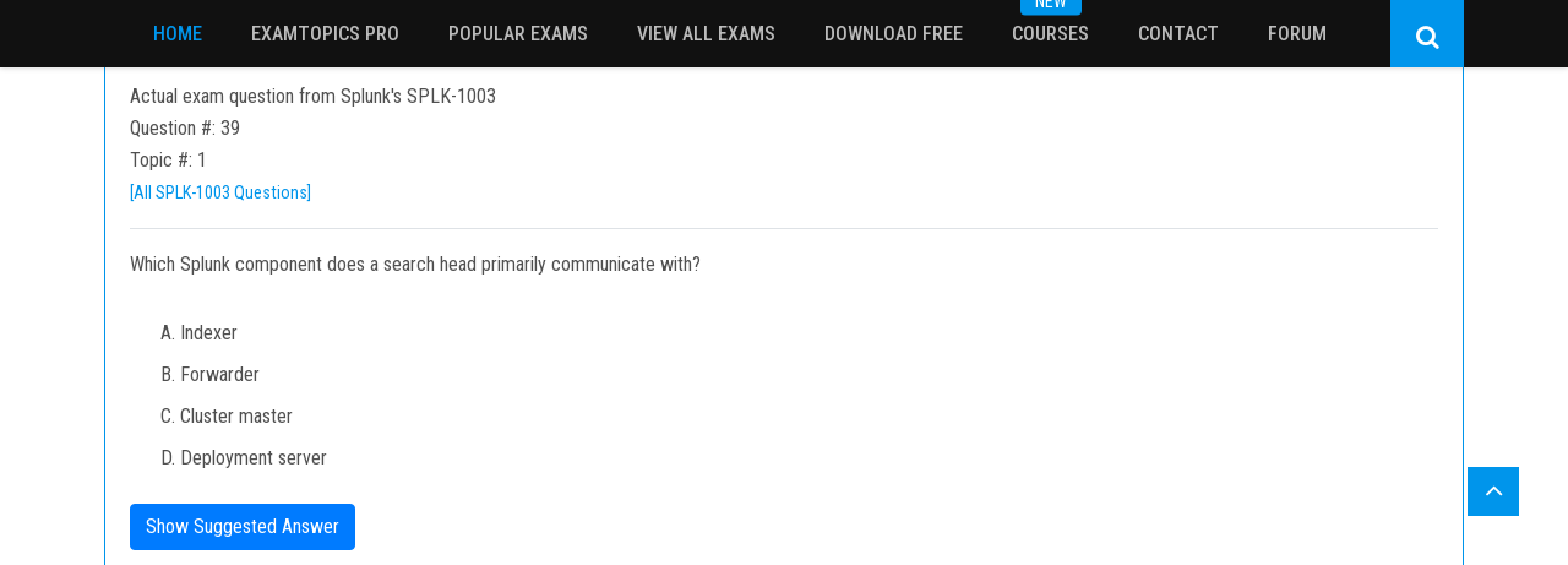
A. True

B. False

C. <regex string>

D. Newline Character

Show Suggested Answer



Actual exam question from Splunk's SPLK-1003

Question #: 39

Topic #: 1

[All SPLK-1003 Questions]

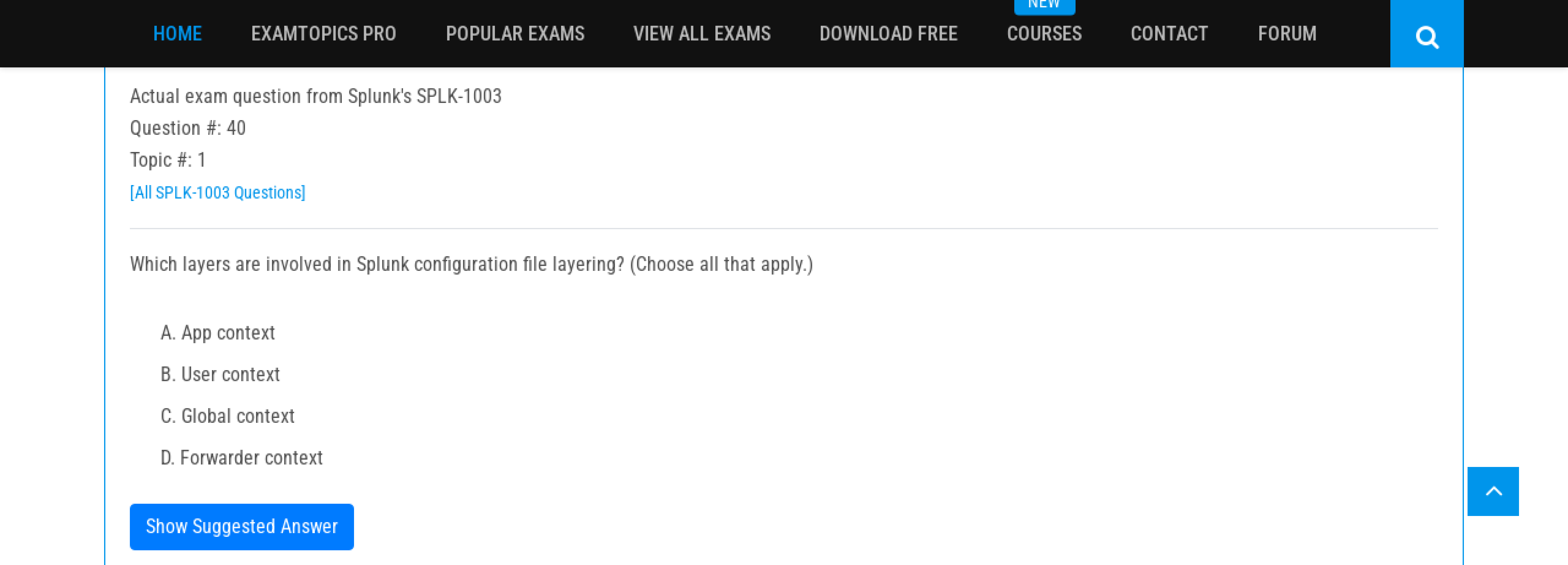
Which Splunk component does a search head primarily communicate with?

A. Indexer

B. Forwarder

C. Cluster master

D. Deployment server



Actual exam question from Splunk's SPLK-1003

Question #: 40

Topic #: 1

[All SPLK-1003 Questions]

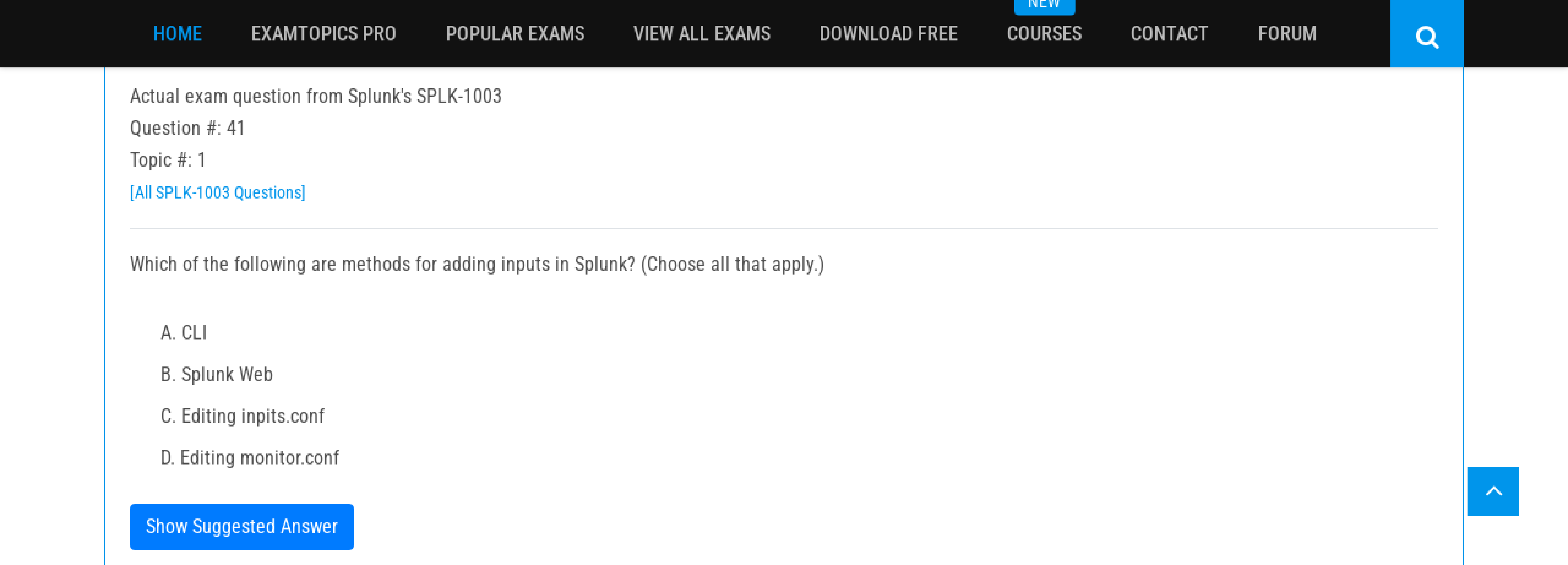
Which layers are involved in Splunk configuration file layering? (Choose all that apply.)

A. App context

B. User context

C. Global context

D. Forwarder context



Actual exam question from Splunk's SPLK-1003

Question #: 41

Topic #: 1

[All SPLK-1003 Questions]

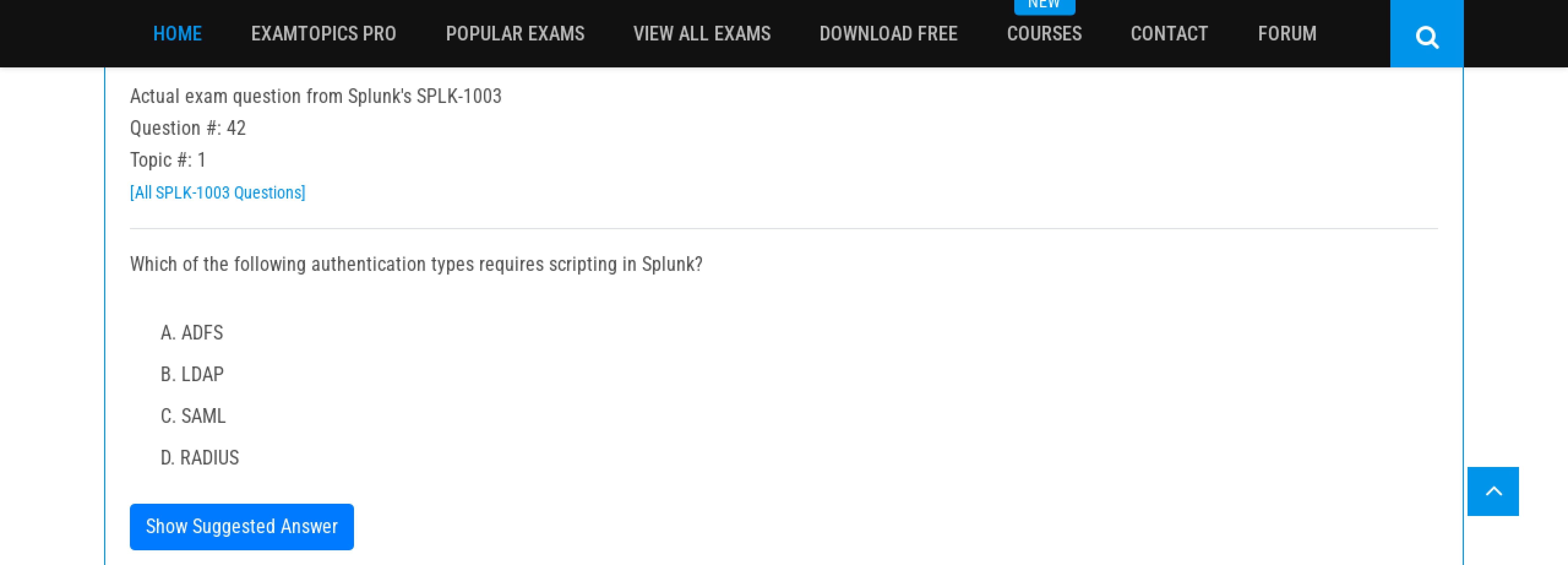
Which of the following are methods for adding inputs in Splunk? (Choose all that apply.)

A. CLI

B. Splunk Web

C. Editing inpits.conf

D. Editing monitor.conf



Actual exam question from Splunk's SPLK-1003

Question #: 42

Topic #: 1

[All SPLK-1003 Questions]

Which of the following authentication types requires scripting in Splunk?

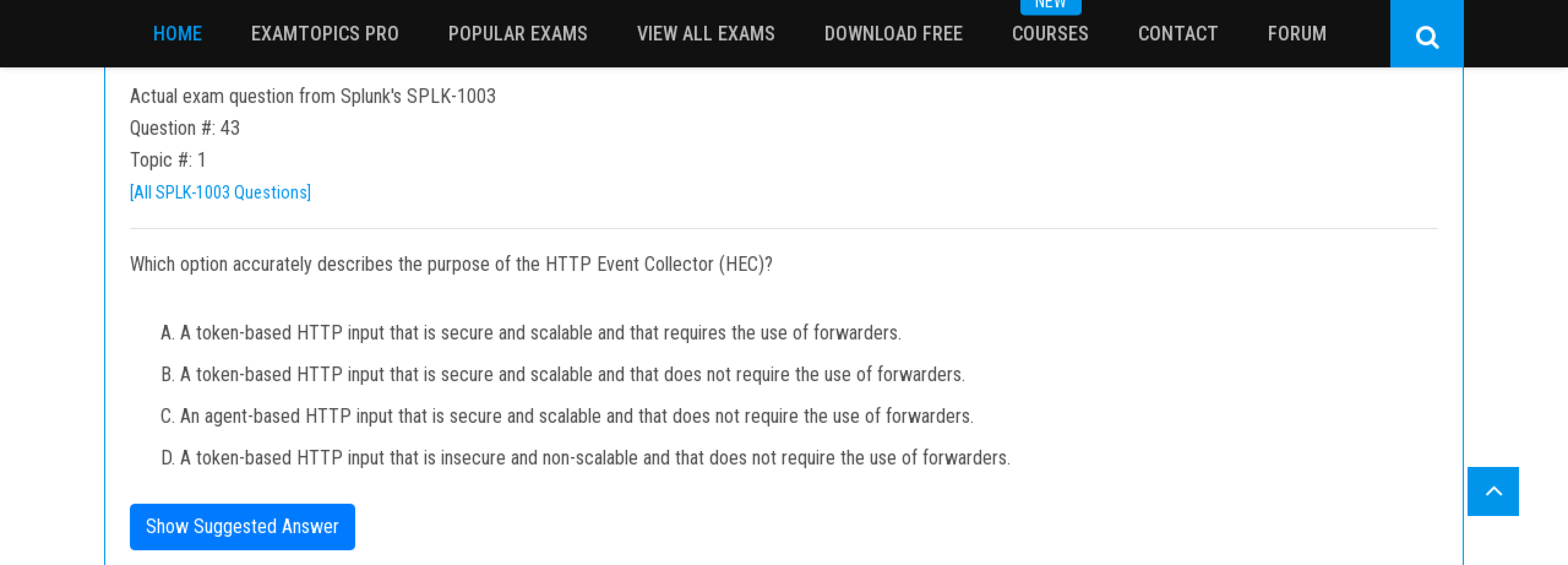
A. ADFS

B. LDAP

C. SAML

D. RADIUS

Show Suggested Answer



Actual exam question from Splunk's SPLK-1003

Question #: 43

Topic #: 1

[All SPLK-1003 Questions]

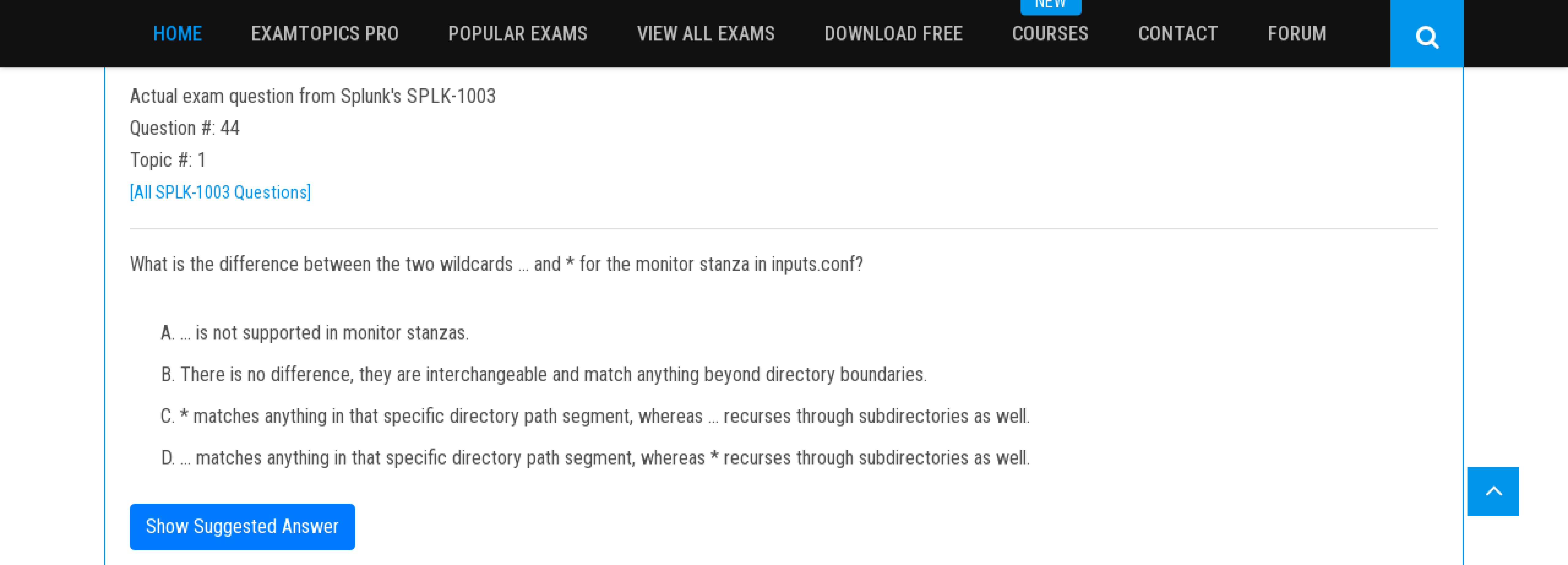
Which option accurately describes the purpose of the HTTP Event Collector (HEC)?

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.



Actual exam question from Splunk's SPLK-1003

Question #: 44

Topic #: 1

[All SPLK-1003 Questions]

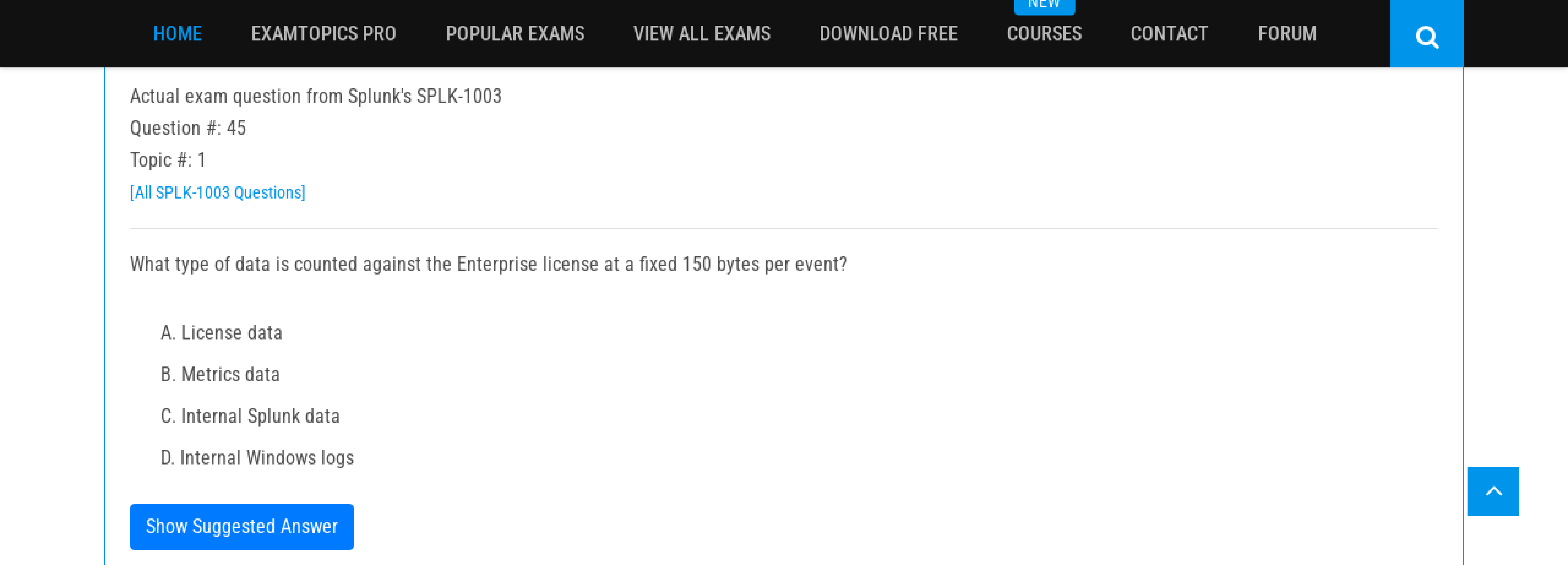
What is the difference between the two wildcards ... and * for the monitor stanza in inputs.conf?

A. ... is not supported in monitor stanzas.

B. There is no difference, they are interchangeable and match anything beyond directory boundaries.

C. * matches anything in that specific directory path segment, whereas ... recurses through subdirectories as well.

D. ... matches anything in that specific directory path segment, whereas * recurses through subdirectories as well.



Actual exam question from Splunk's SPLK-1003

Question #: 45

Topic #: 1

[All SPLK-1003 Questions]

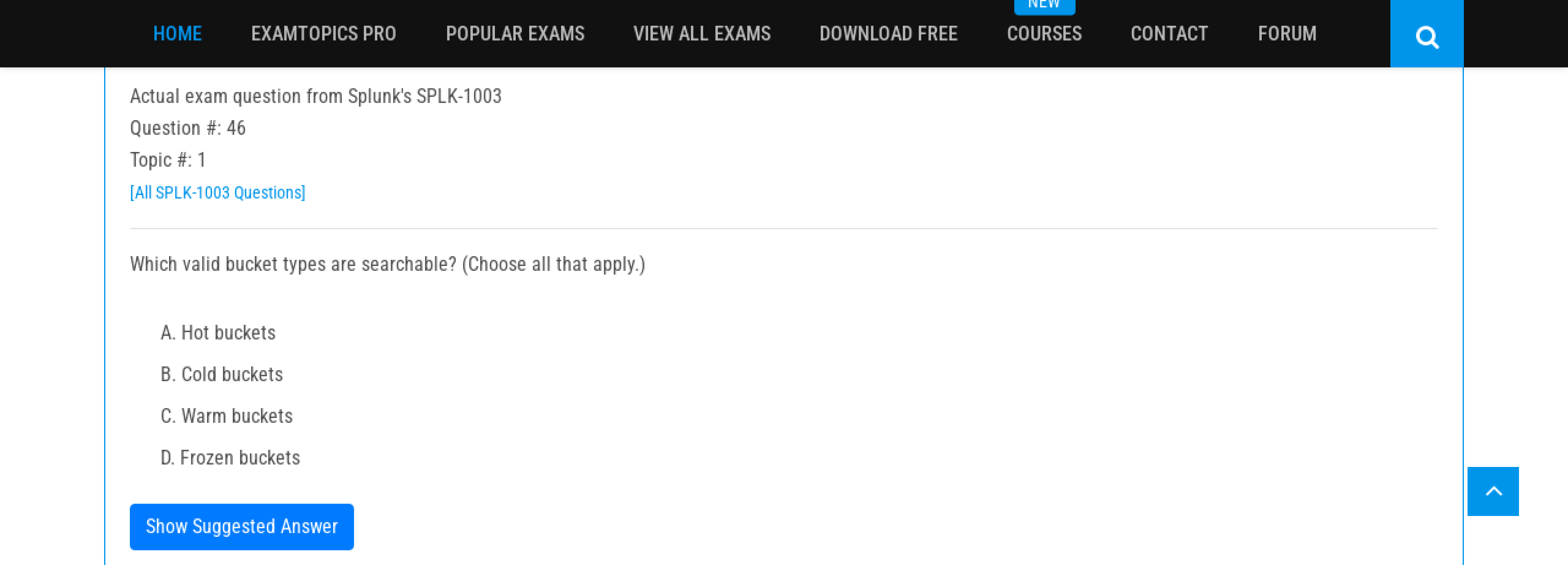
What type of data is counted against the Enterprise license at a fixed 150 bytes per event?

A. License data

B. Metrics data

C. Internal Splunk data

D. Internal Windows logs



Actual exam question from Splunk's SPLK-1003

Question #: 46

Topic #: 1

[All SPLK-1003 Questions]

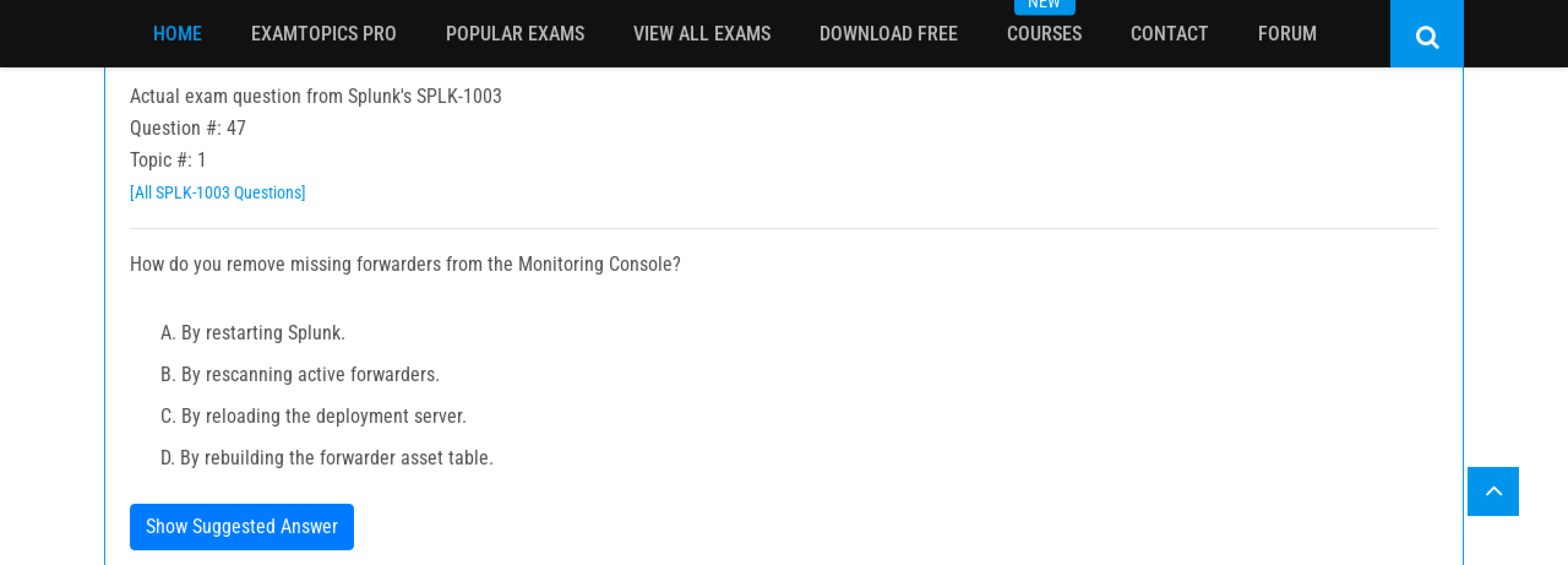
Which valid bucket types are searchable? (Choose all that apply.)

A. Hot buckets

B. Cold buckets

C. Warm buckets

D. Frozen buckets



Actual exam question from Splunk's SPLK-1003

Question #: 47

Topic #: 1

[All SPLK-1003 Questions]

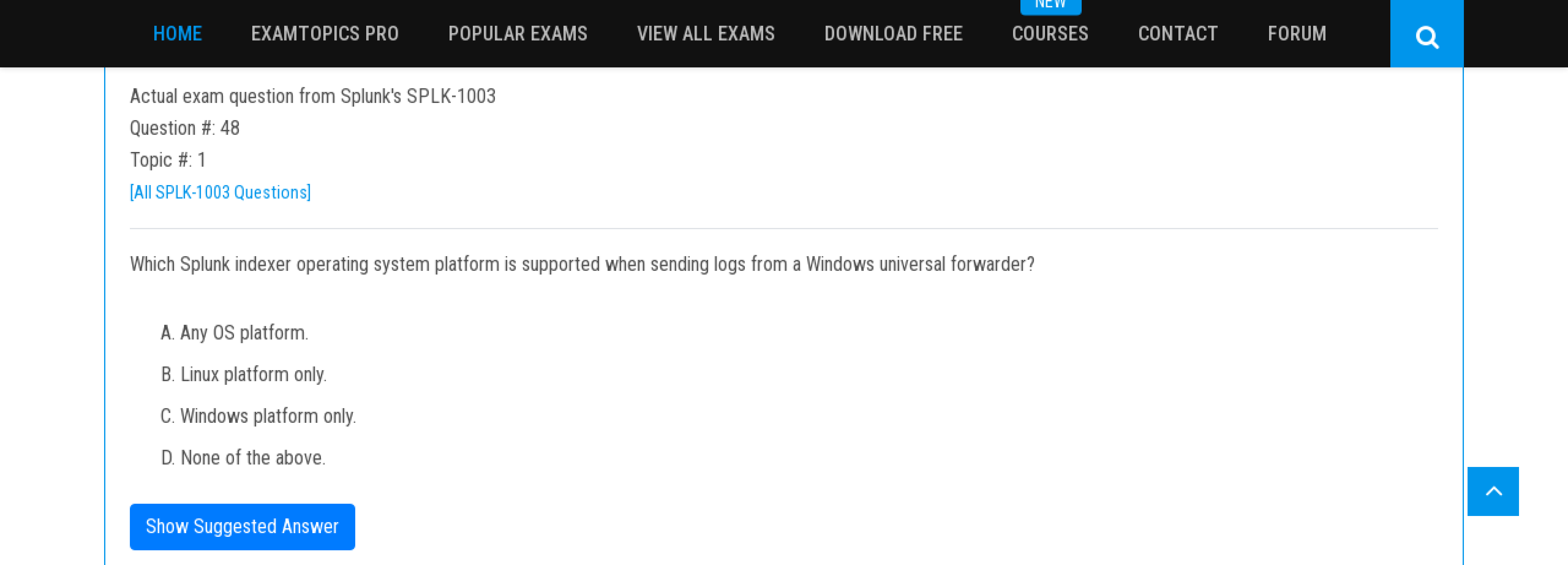
How do you remove missing forwarders from the Monitoring Console?

A. By restarting Splunk.

B. By rescanning active forwarders.

C. By reloading the deployment server.

D. By rebuilding the forwarder asset table.



Actual exam question from Splunk's SPLK-1003

Question #: 48

Topic #: 1

[All SPLK-1003 Questions]

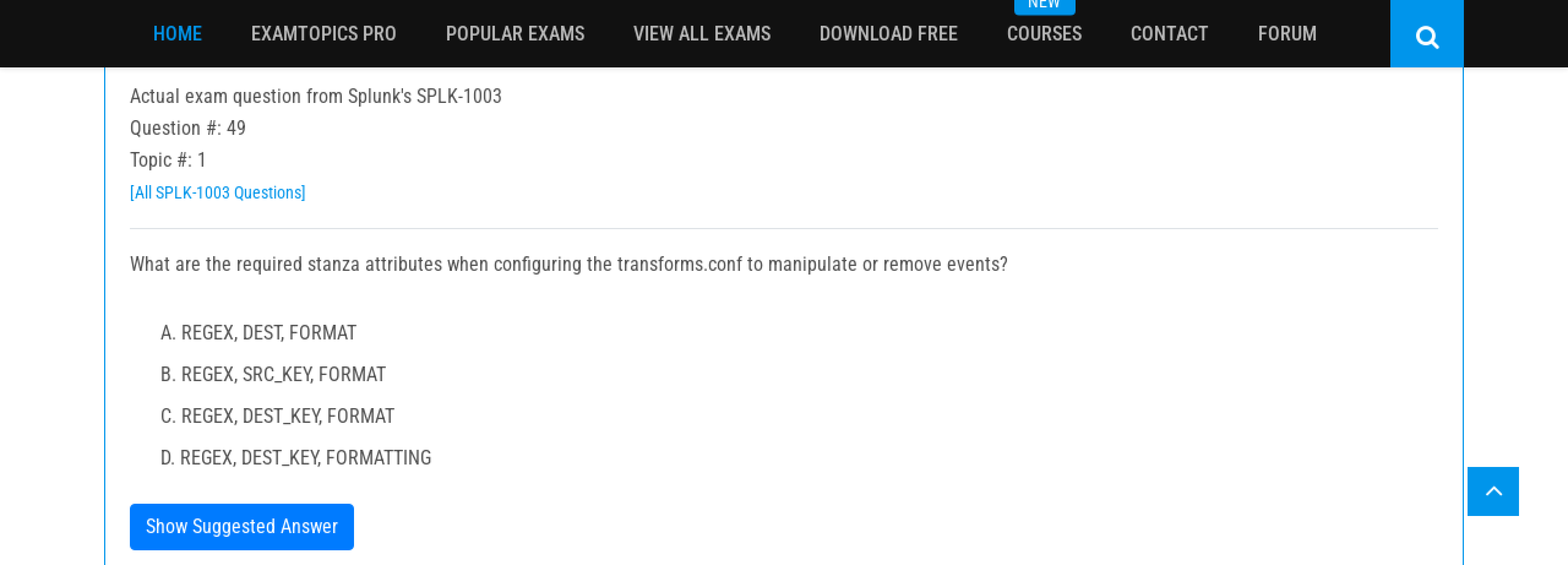
Which Splunk indexer operating system platform is supported when sending logs from a Windows universal forwarder?

A. Any OS platform.

B. Linux platform only.

C. Windows platform only.

D. None of the above.



Actual exam question from Splunk's SPLK-1003

Question #: 49

Topic #: 1

[All SPLK-1003 Questions]

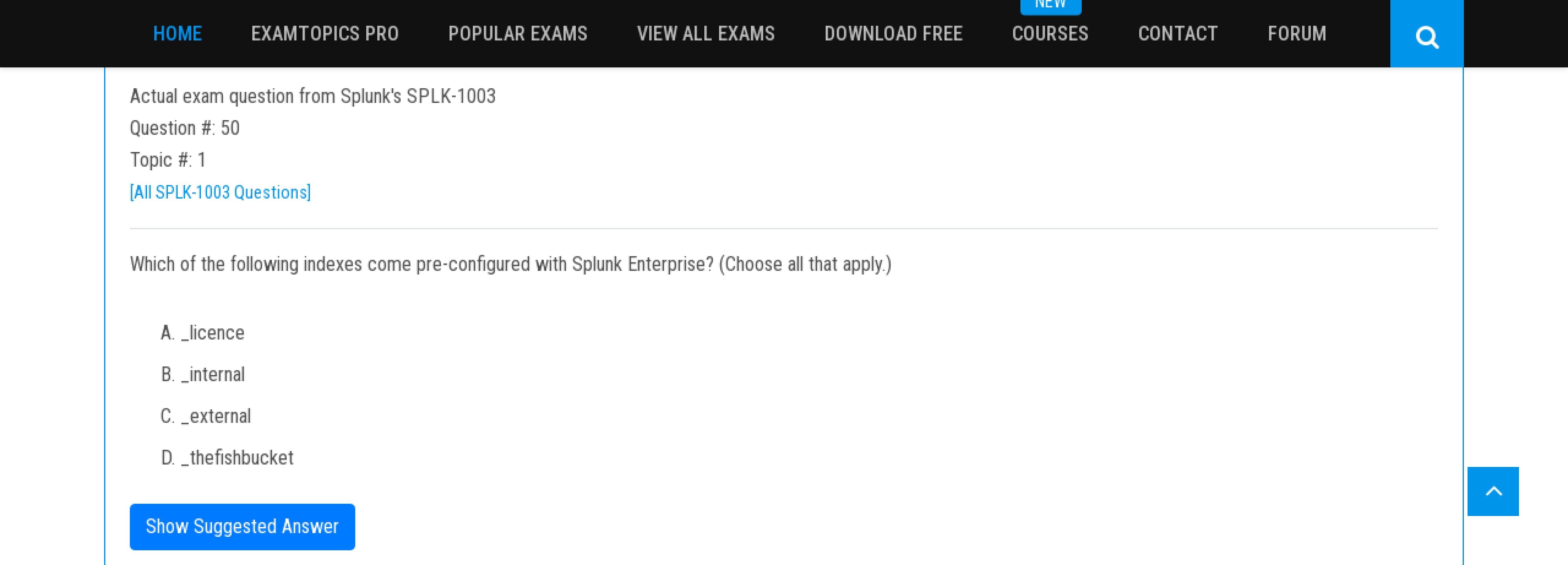
What are the required stanza attributes when configuring the transforms.conf to manipulate or remove events?

A. REGEX, DEST, FORMAT

B. REGEX, SRC_KEY, FORMAT

C. REGEX, DEST_KEY, FORMAT

D. REGEX, DEST_KEY, FORMATTING



Actual exam question from Splunk's SPLK-1003

Question #: 50

Topic #: 1

[All SPLK-1003 Questions]

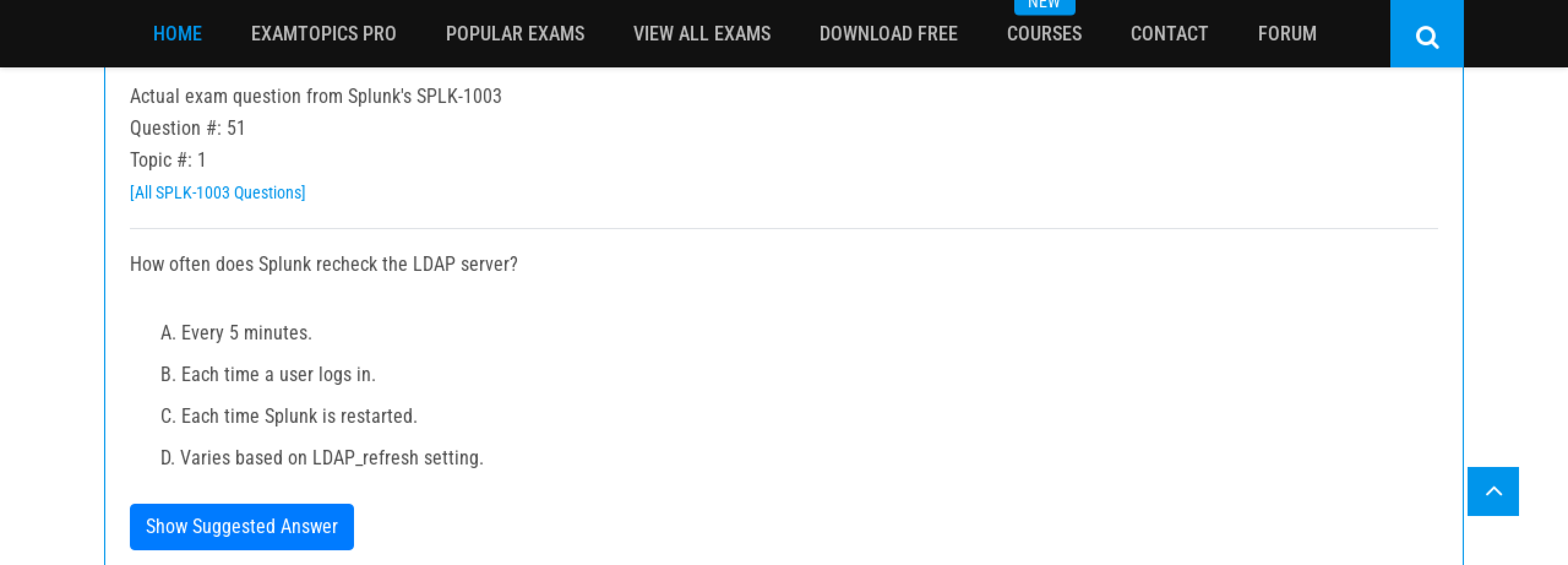
Which of the following indexes come pre-configured with Splunk Enterprise? (Choose all that apply.)

A. _licence

B. _internal

C. _external

D. _thefishbucket



Actual exam question from Splunk's SPLK-1003

Question #: 51

Topic #: 1

[All SPLK-1003 Questions]

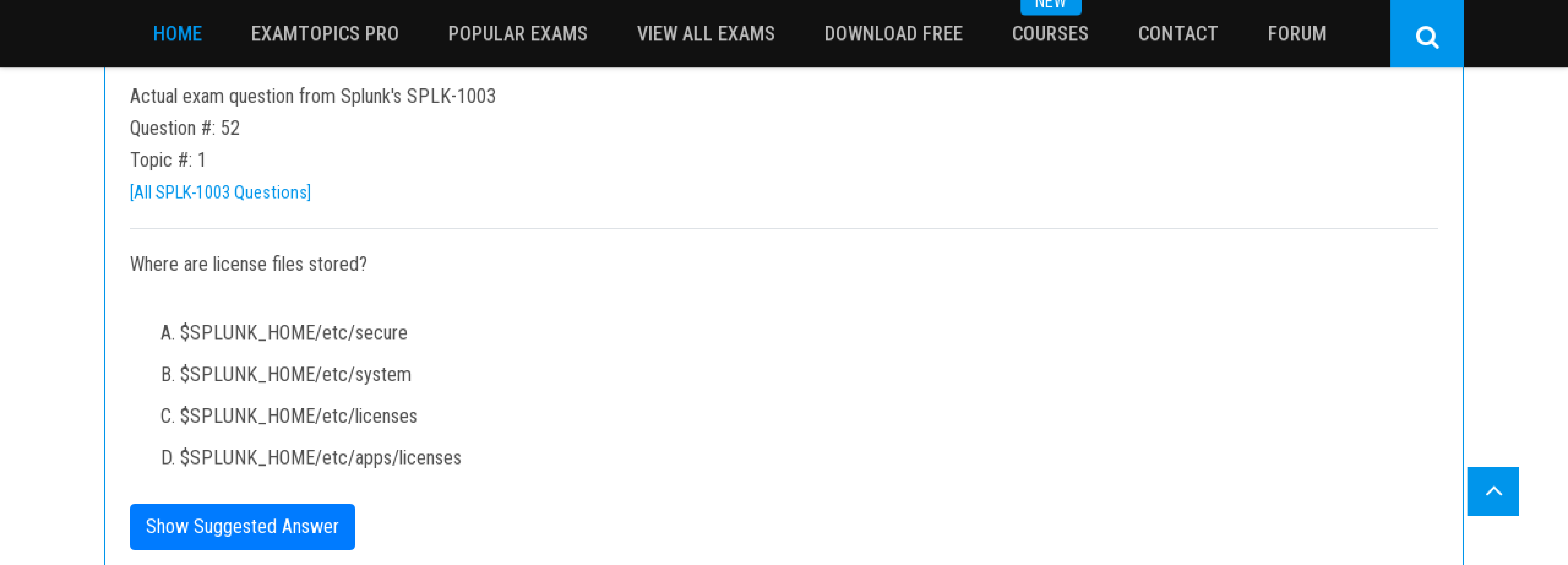
How often does Splunk recheck the LDAP server?

A. Every 5 minutes.

B. Each time a user logs in.

C. Each time Splunk is restarted.

D. Varies based on LDAP_refresh setting.



Actual exam question from Splunk's SPLK-1003

Question #: 52

Topic #: 1

[All SPLK-1003 Questions]

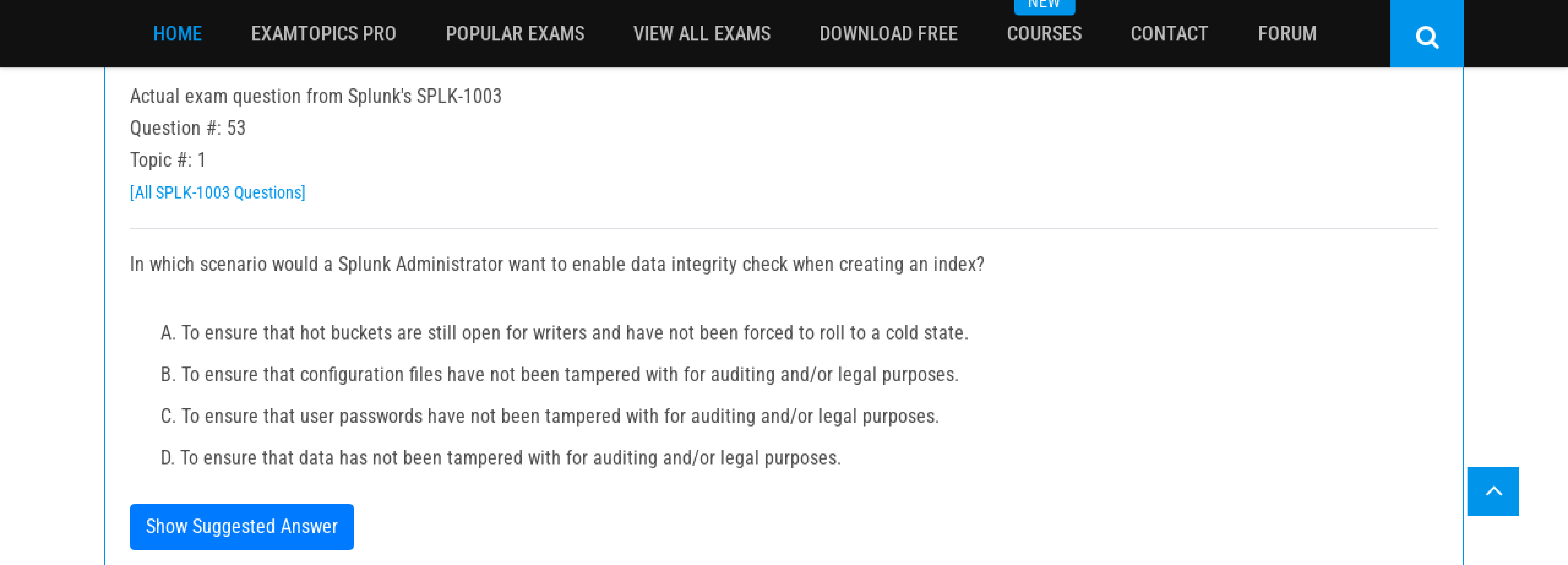
Where are license files stored?

A. $SPLUNK_HOME/etc/secure

B. $SPLUNK_HOME/etc/system

C. $SPLUNK_HOME/etc/licenses

D. $SPLUNK_HOME/etc/apps/licenses



Actual exam question from Splunk's SPLK-1003

Question #: 53

Topic #: 1

[All SPLK-1003 Questions]

In which scenario would a Splunk Administrator want to enable data integrity check when creating an index?

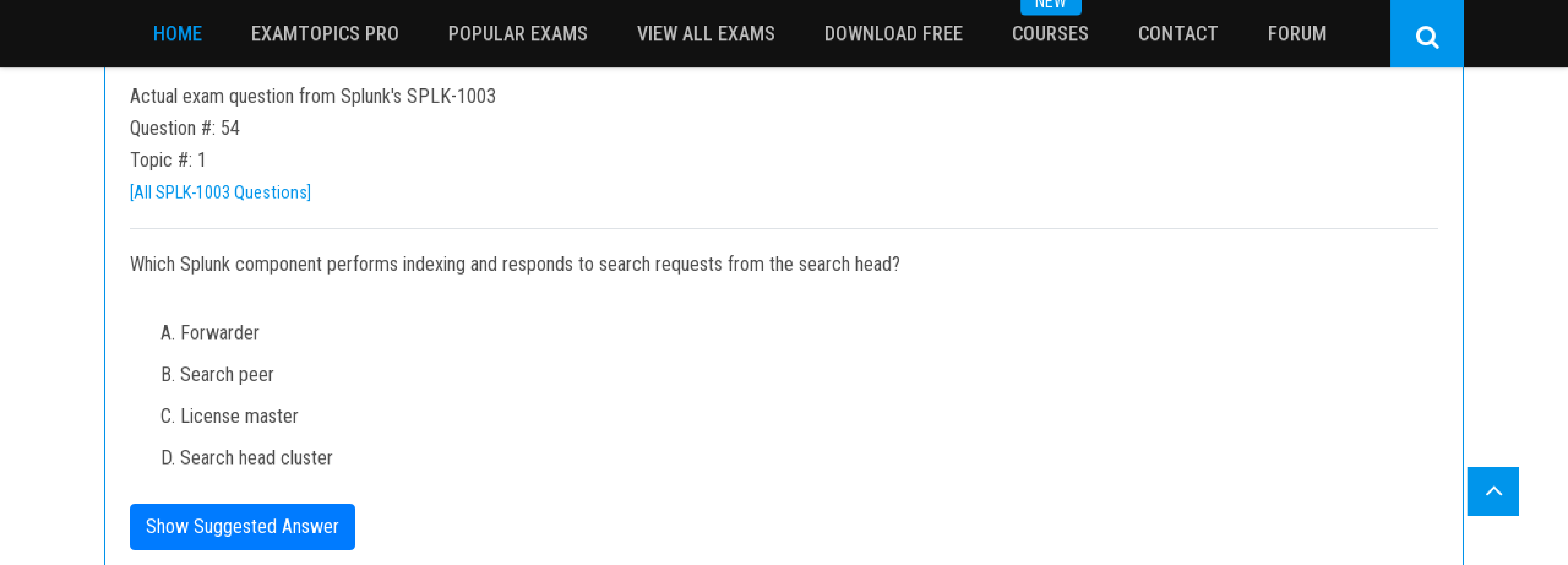
A. To ensure that hot buckets are still open for writers and have not been forced to roll to a cold state.

B. To ensure that configuration files have not been tampered with for auditing and/or legal purposes.

C. To ensure that user passwords have not been tampered with for auditing and/or legal purposes.

D. To ensure that data has not been tampered with for auditing and/or legal purposes.

Show Suggested Answer



Actual exam question from Splunk's SPLK-1003

Question #: 54

Topic #: 1

[All SPLK-1003 Questions]

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

Show Suggested Answer

Actual exam question from Splunk's SPLK-1003

Question #: 55

Topic #: 1

[All SPLK-1003 Questions]

When deploying apps, which attribute in the forwarder management interface determines the apps that clients install?

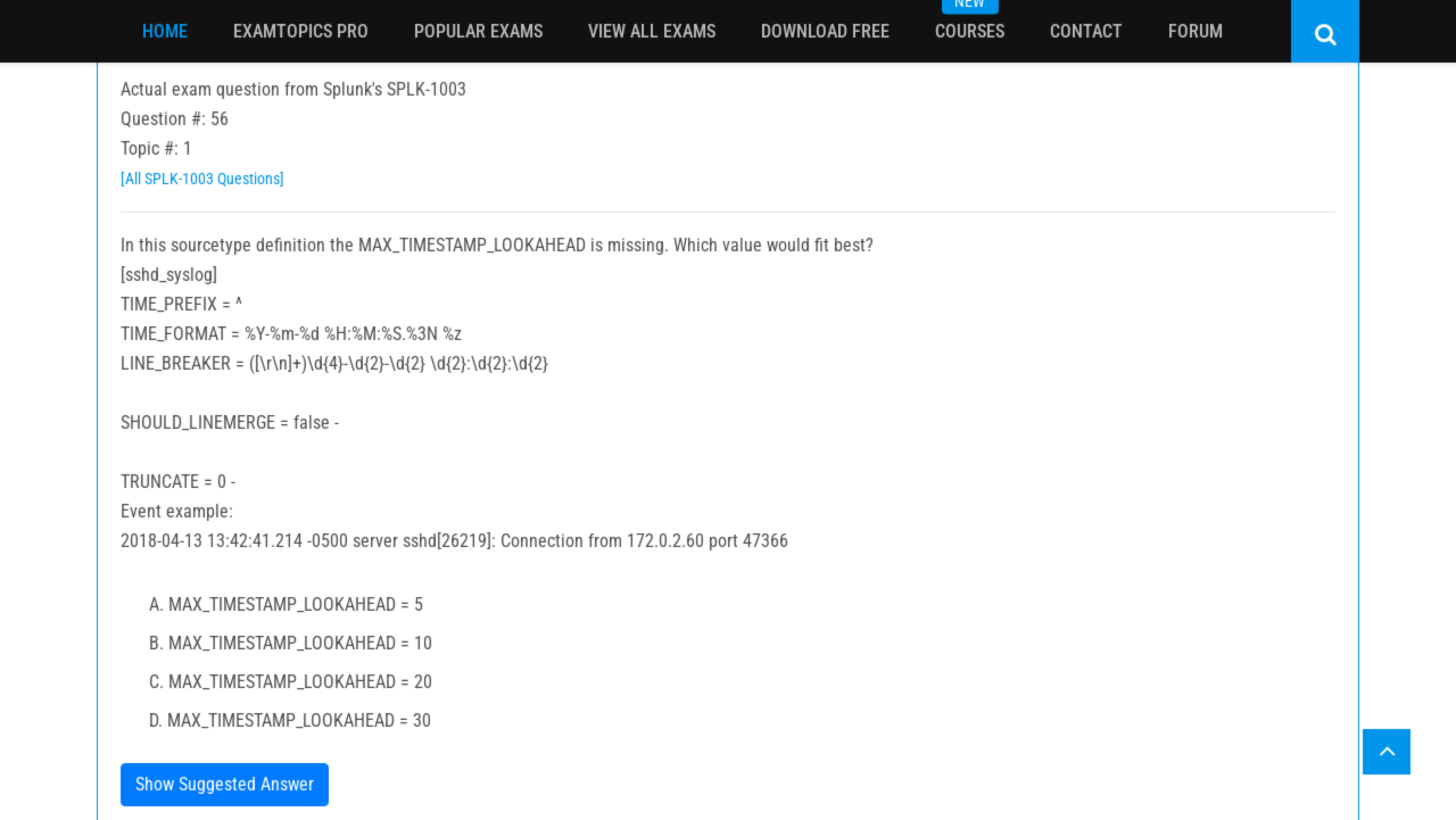
A. App Class

B. Client Class

C. Server Class

D. Forwarder Class

Show Suggested Answer



Actual exam question from Splunk's SPLK-1003

Question #: 56

Topic #: 1

[All SPLK-1003 Questions]

In this sourcetype definition the MAX_TIMESTAMP_LOOKAHEAD is missing. Which value would fit best?

```
[sshd_syslog]
TIME_PREFIX = ^
TIME_FORMAT = %Y-%m-%d %H:%M:%S.%3N %z
LINE_BREAKER = ([\r\n]+)\d{4}-\d{2}-\d{2} \d{2}:\d{2}:\d{2}

SHOULD_LINEMERGE = false -

TRUNCATE = 0 -
```

Event example:

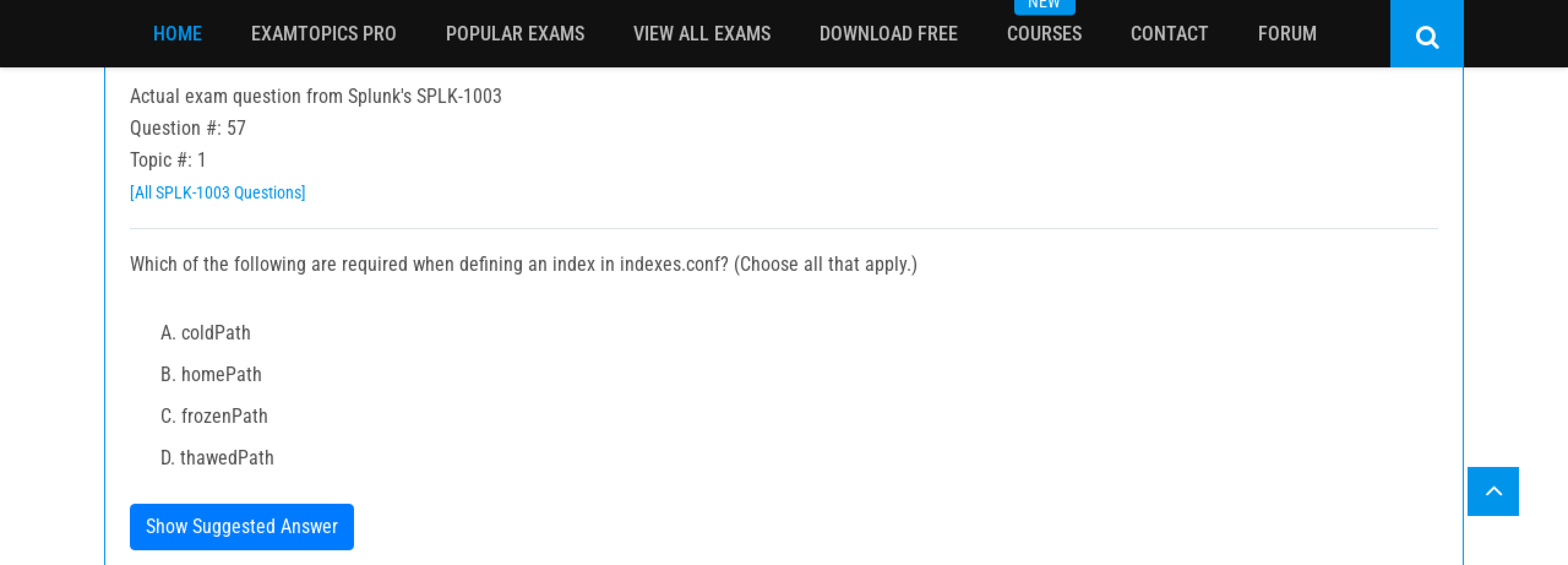
```
2018-04-13 13:42:41.214 -0500 server sshd[26219]: Connection from 172.0.2.60 port 47366
```

A. MAX_TIMESTAMP_LOOKAHEAD = 5

B. MAX_TIMESTAMP_LOOKAHEAD = 10

C. MAX_TIMESTAMP_LOOKAHEAD = 20

D. MAX_TIMESTAMP_LOOKAHEAD = 30



Actual exam question from Splunk's SPLK-1003

Question #: 57

Topic #: 1

[All SPLK-1003 Questions]

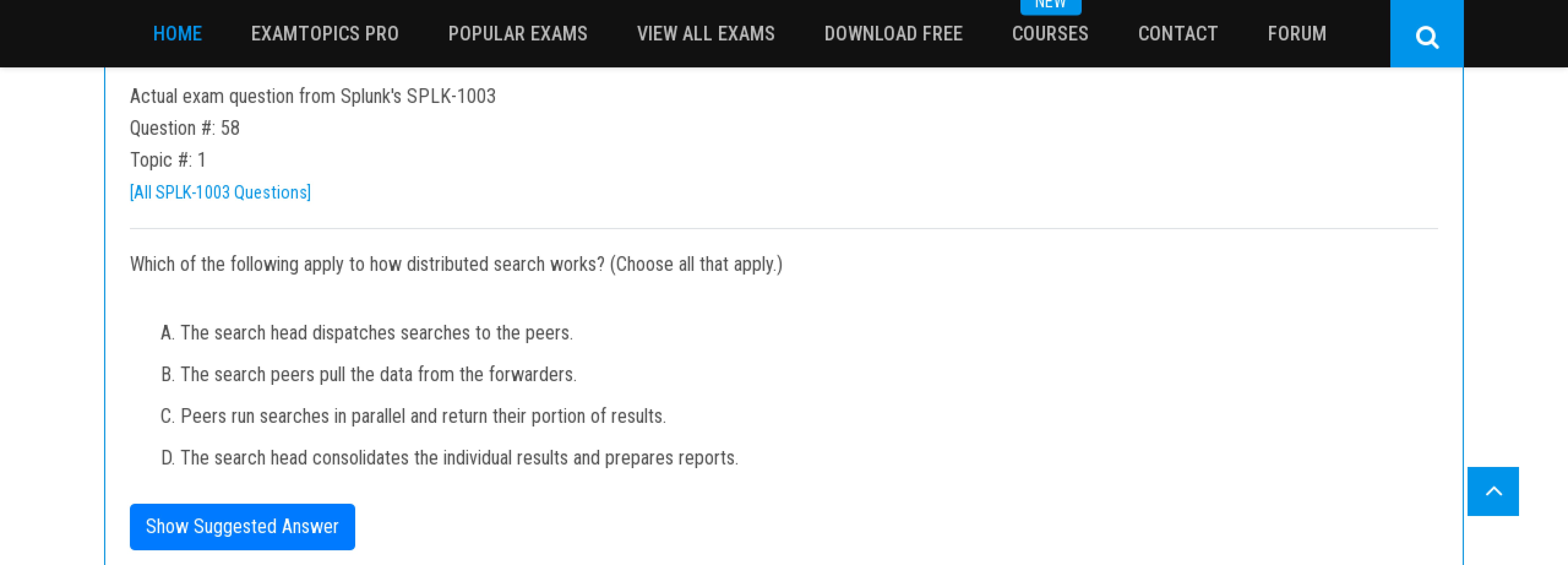
Which of the following are required when defining an index in indexes.conf? (Choose all that apply.)

A. coldPath

B. homePath

C. frozenPath

D. thawedPath



Actual exam question from Splunk's SPLK-1003

Question #: 58

Topic #: 1

[All SPLK-1003 Questions]

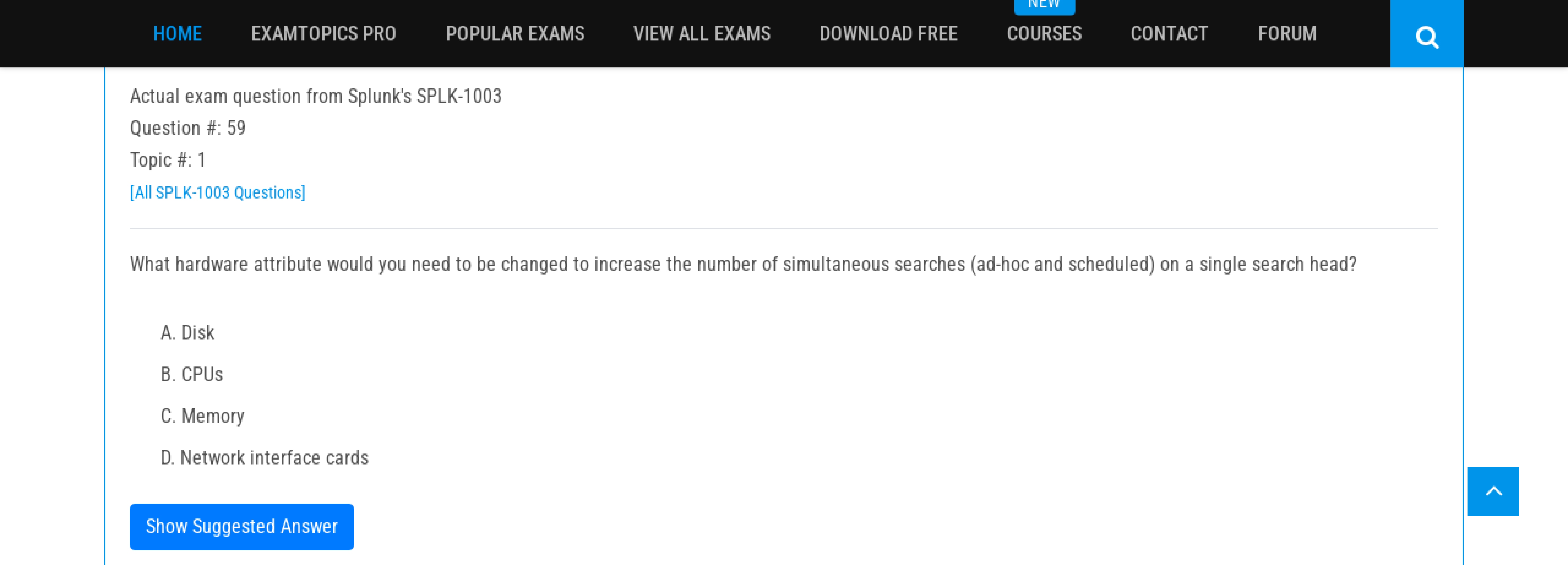
Which of the following apply to how distributed search works? (Choose all that apply.)

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.



Actual exam question from Splunk's SPLK-1003

Question #: 59

Topic #: 1

[All SPLK-1003 Questions]

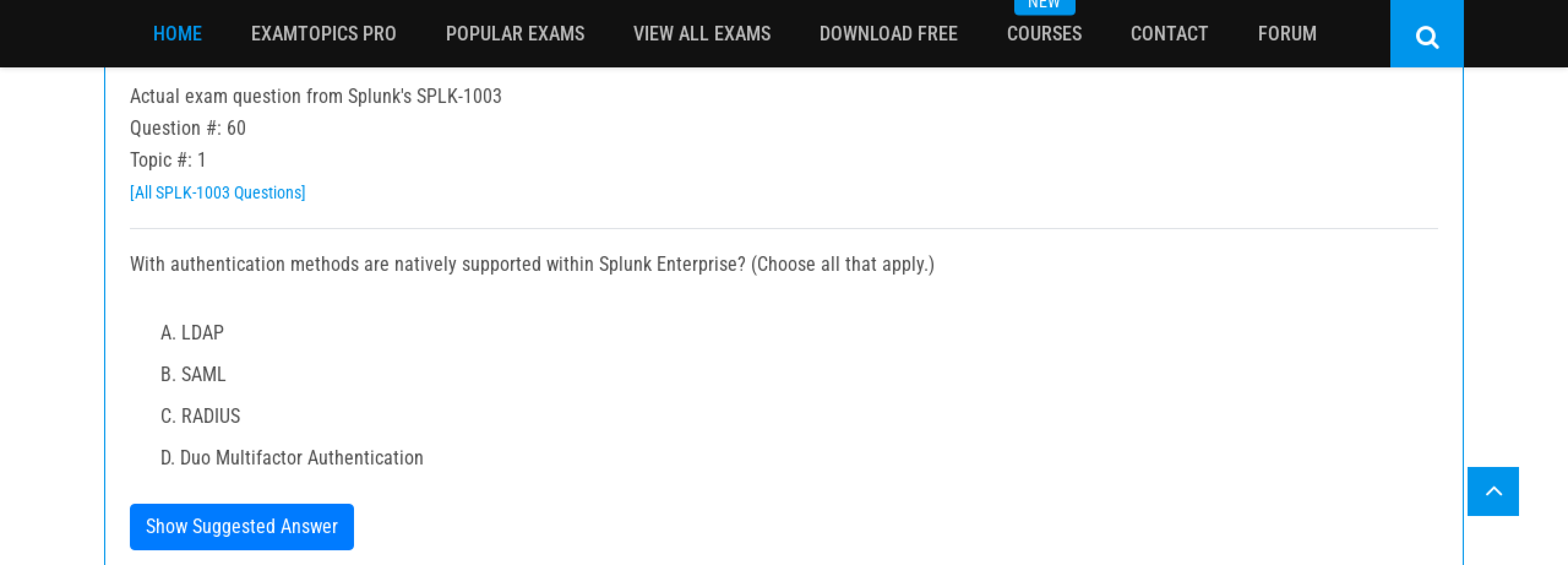
What hardware attribute would you need to be changed to increase the number of simultaneous searches (ad-hoc and scheduled) on a single search head?

A. Disk

B. CPUs

C. Memory

D. Network interface cards



Actual exam question from Splunk's SPLK-1003

Question #: 60

Topic #: 1

[All SPLK-1003 Questions]

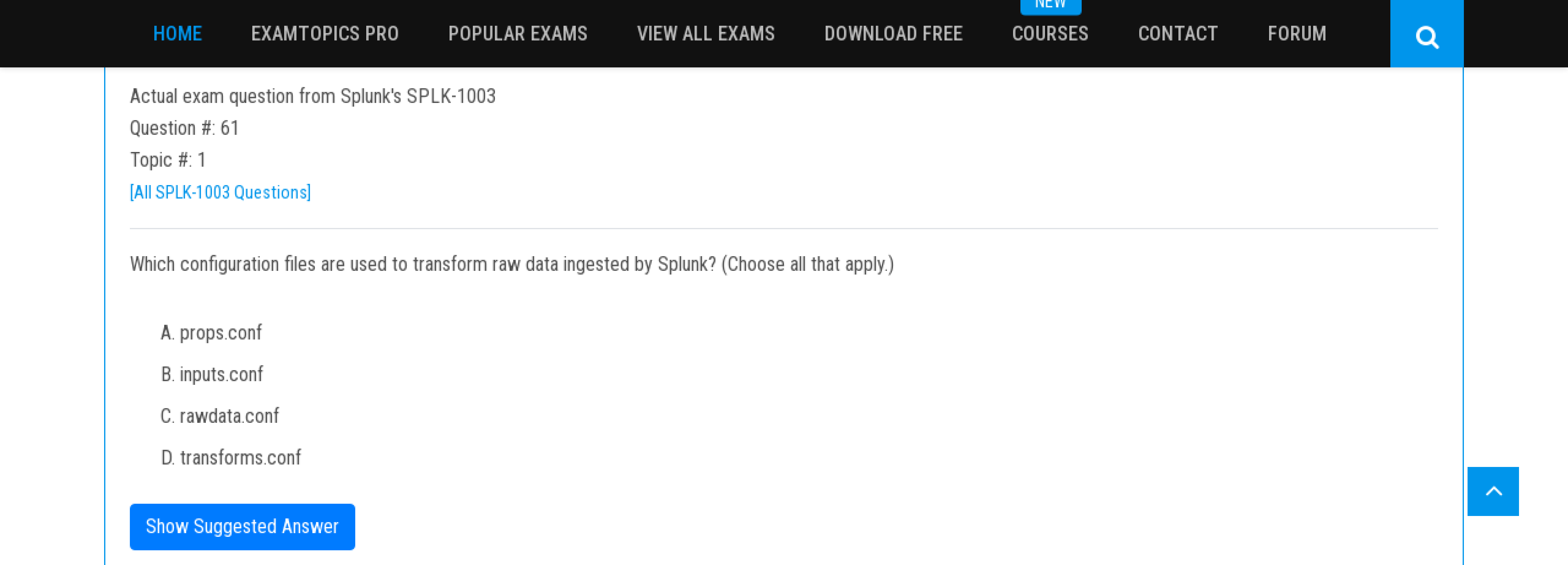
With authentication methods are natively supported within Splunk Enterprise? (Choose all that apply.)

A. LDAP

B. SAML

C. RADIUS

D. Duo Multifactor Authentication



Actual exam question from Splunk's SPLK-1003

Question #: 61

Topic #: 1

[All SPLK-1003 Questions]

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

Actual exam question from Splunk's SPLK-1003

Question #: 62

Topic #: 1

[All SPLK-1003 Questions]

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

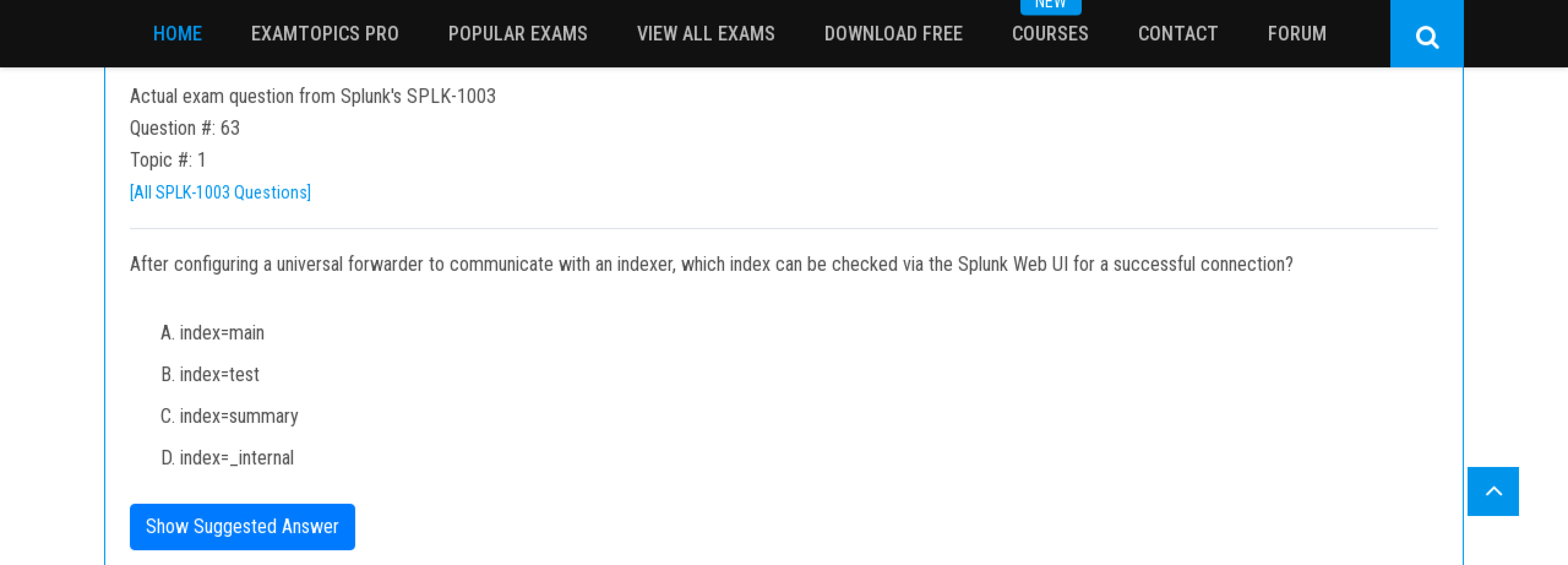
A. props.conf

B. search.conf

C. distsearch.conf

D. distibutedsearch.conf

Show Suggested Answer



Actual exam question from Splunk's SPLK-1003

Question #: 63

Topic #: 1

[All SPLK-1003 Questions]

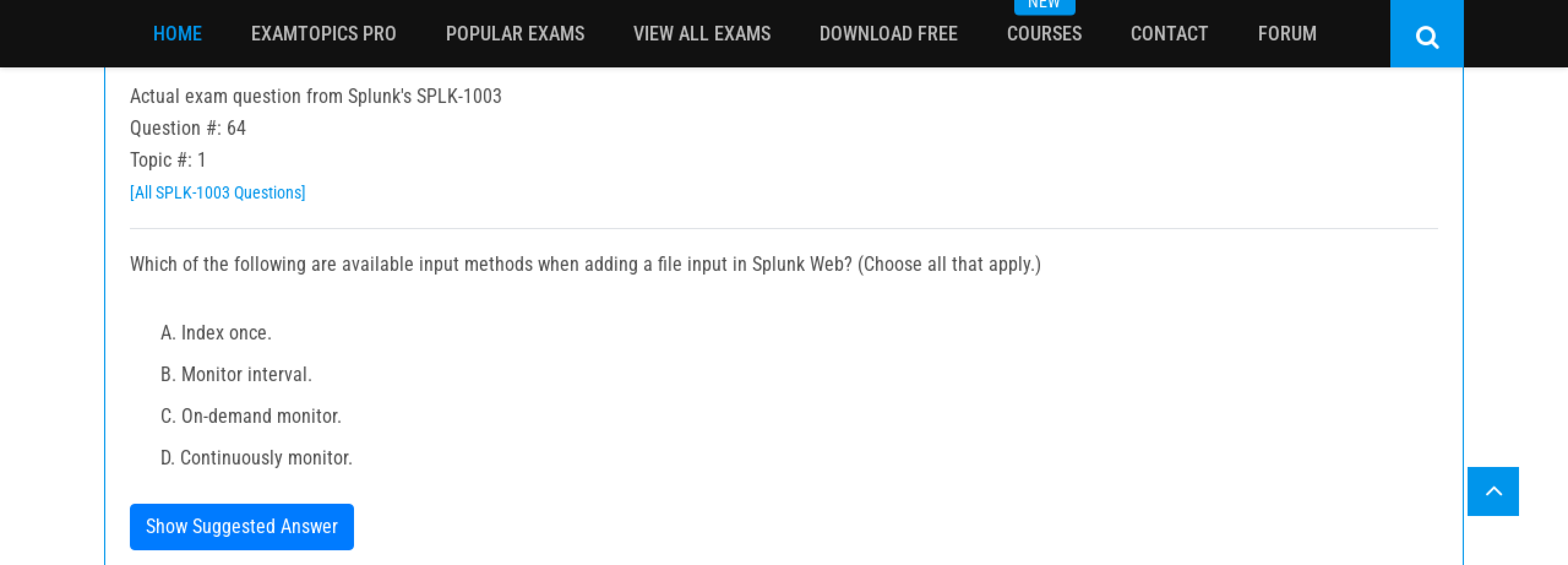
After configuring a universal forwarder to communicate with an indexer, which index can be checked via the Splunk Web UI for a successful connection?

A. index=main

B. index=test

C. index=summary

D. index=_internal



Actual exam question from Splunk's SPLK-1003

Question #: 64

Topic #: 1

[All SPLK-1003 Questions]

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

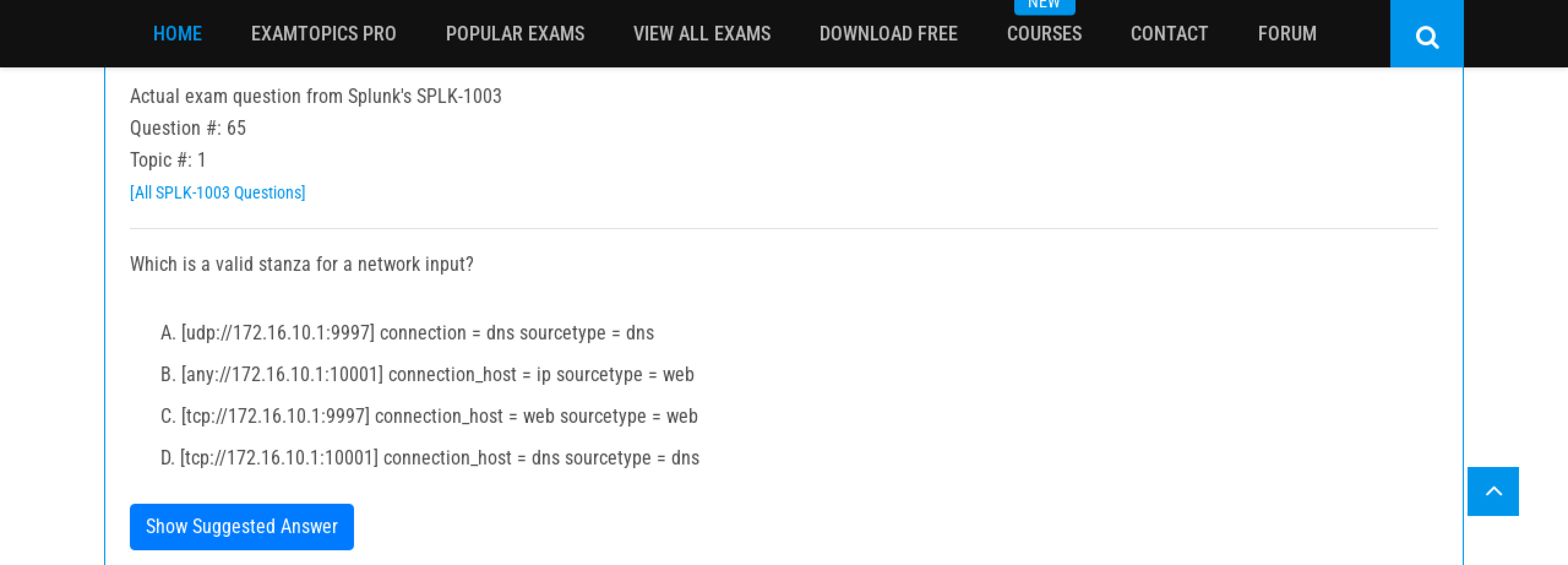
A. Index once.

B. Monitor interval.

C. On-demand monitor.

D. Continuously monitor.

Show Suggested Answer



Actual exam question from Splunk's SPLK-1003

Question #: 65

Topic #: 1

[All SPLK-1003 Questions]

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

Actual exam question from Splunk's SPLK-1003

Question #: 66

Topic #: 1

[All SPLK-1003 Questions]

Which additional component is required for a search head cluster?

A. Deployer

B. Cluster Master

C. Monitoring Console

D. Management Console

Show Suggested Answer

Actual exam question from Splunk's SPLK-1003

Question #: 67

Topic #: 1

[All SPLK-1003 Questions]

When are knowledge bundles distributed to search peers?

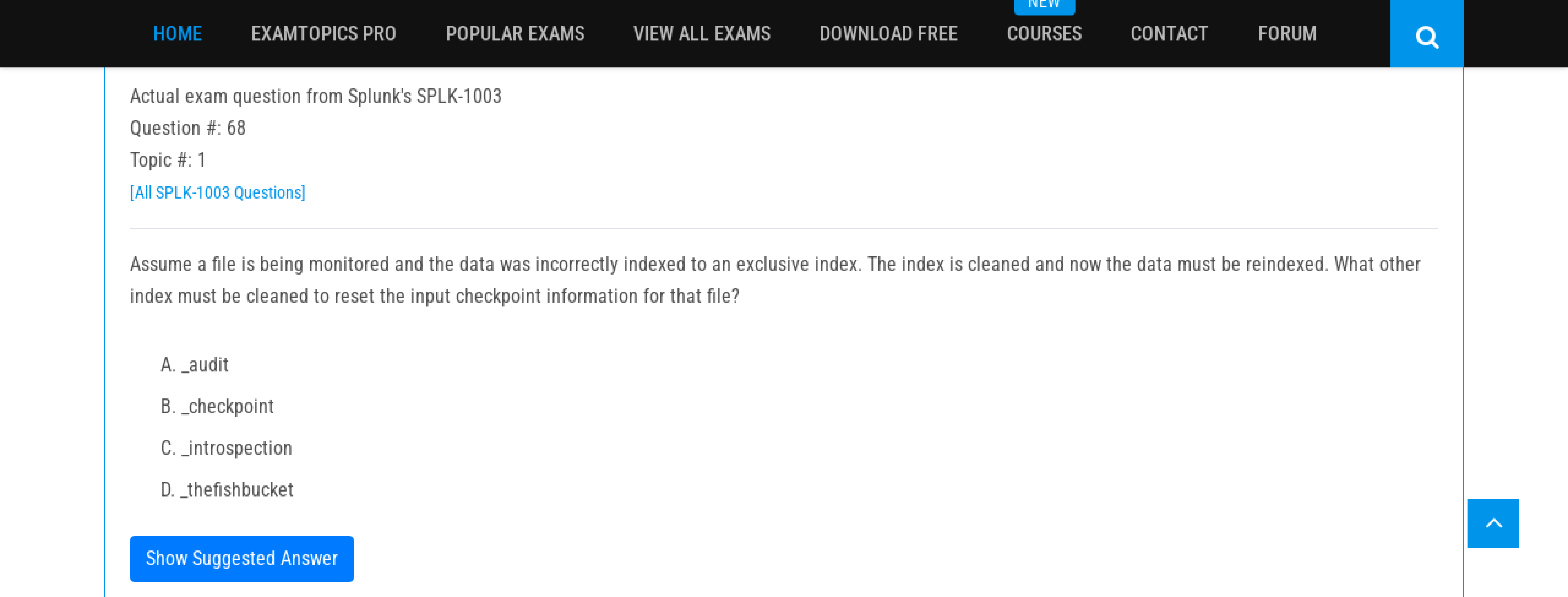
A. After a user logs in.

B. When Splunk is restarted.

C. When adding a new search peer.

D. When a distributed search is initiated.

Show Suggested Answer



Actual exam question from Splunk's SPLK-1003

Question #: 68

Topic #: 1

[All SPLK-1003 Questions]

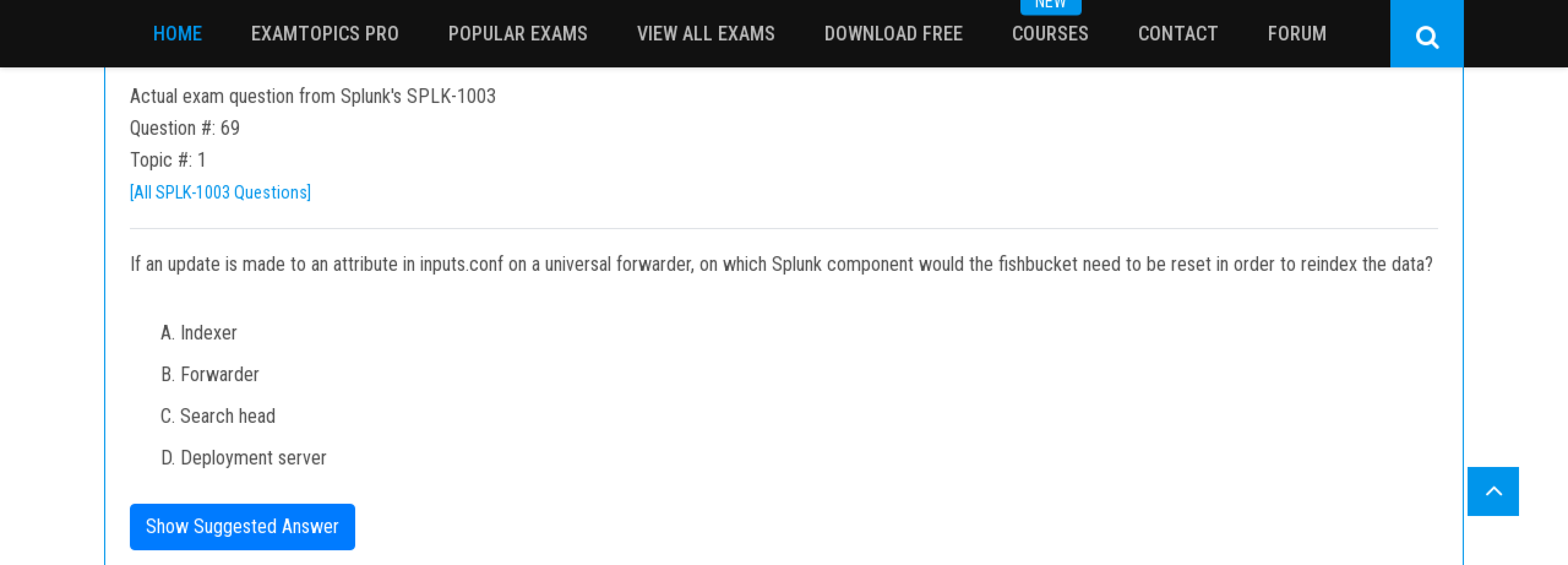
Assume a file is being monitored and the data was incorrectly indexed to an exclusive index. The index is cleaned and now the data must be reindexed. What other index must be cleaned to reset the input checkpoint information for that file?

A. _audit

B. _checkpoint

C. _introspection

D. _thefishbucket



Actual exam question from Splunk's SPLK-1003

Question #: 69

Topic #: 1

[All SPLK-1003 Questions]

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?

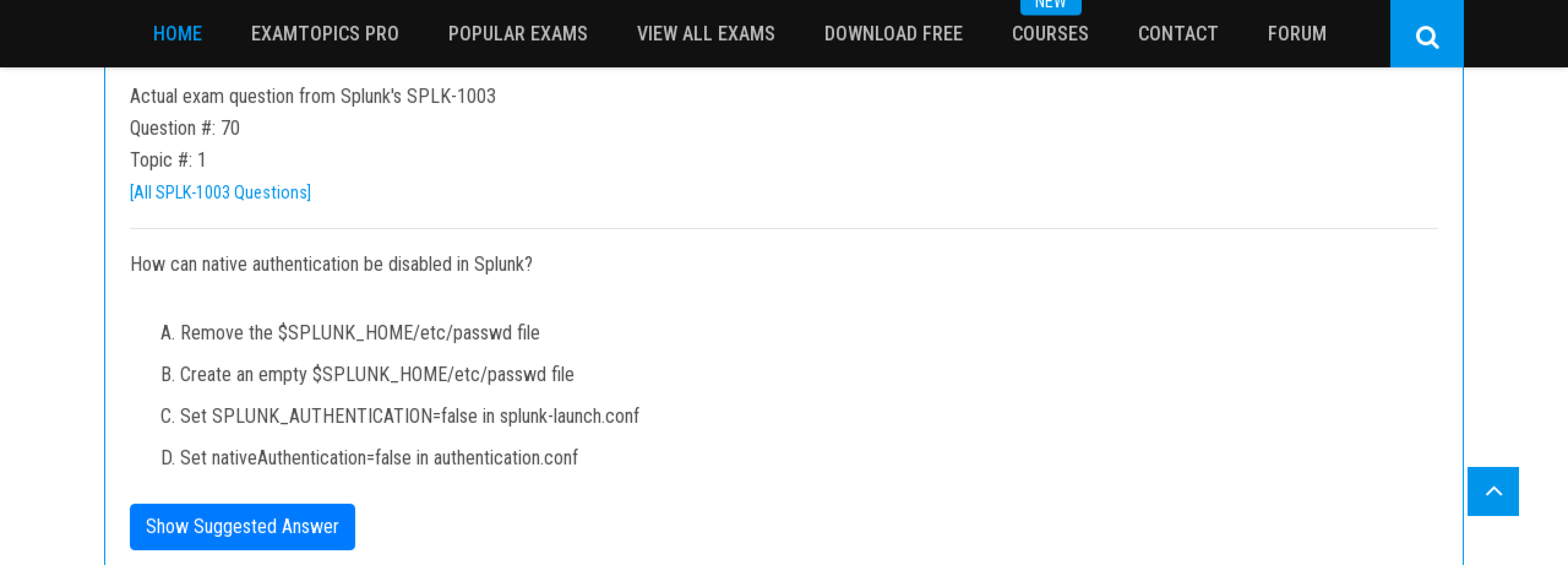
A. Indexer

B. Forwarder

C. Search head

D. Deployment server

Show Suggested Answer



Actual exam question from Splunk's SPLK-1003

Question #: 70

Topic #: 1

[All SPLK-1003 Questions]

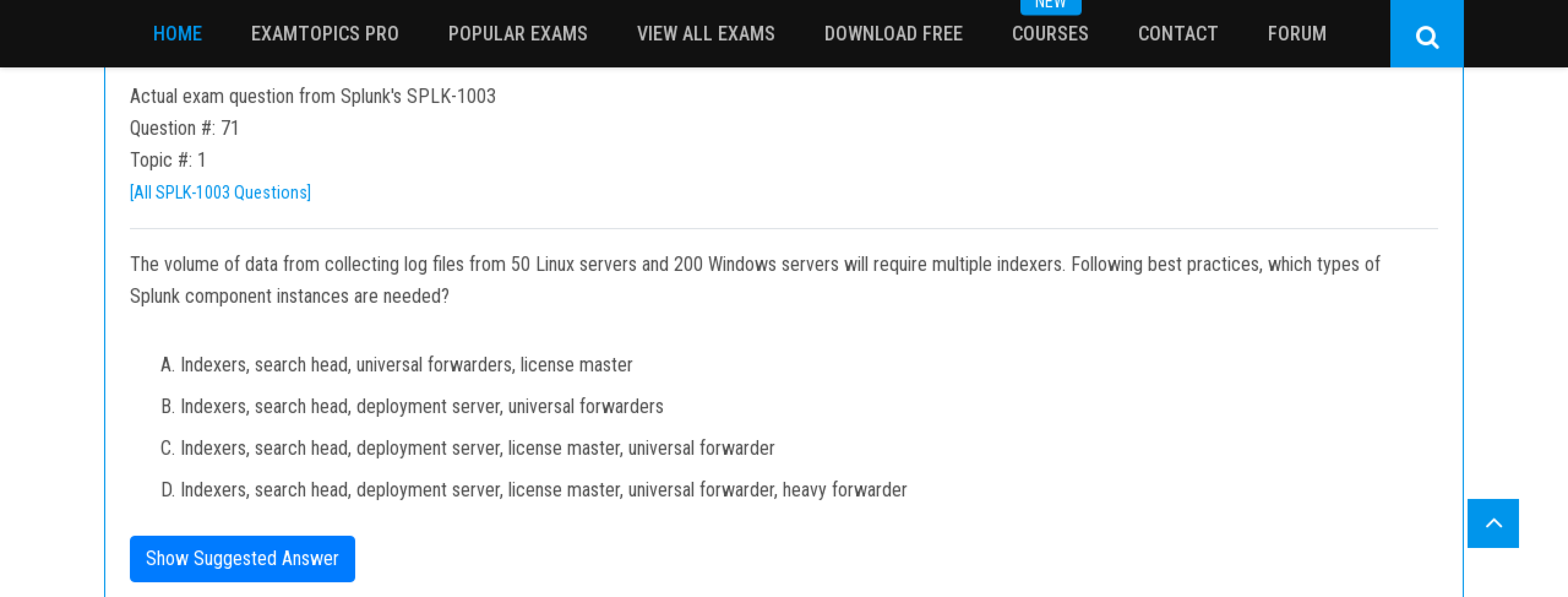
How can native authentication be disabled in Splunk?

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



Actual exam question from Splunk's SPLK-1003
Question #: 71
Topic #: 1
[All SPLK-1003 Questions]

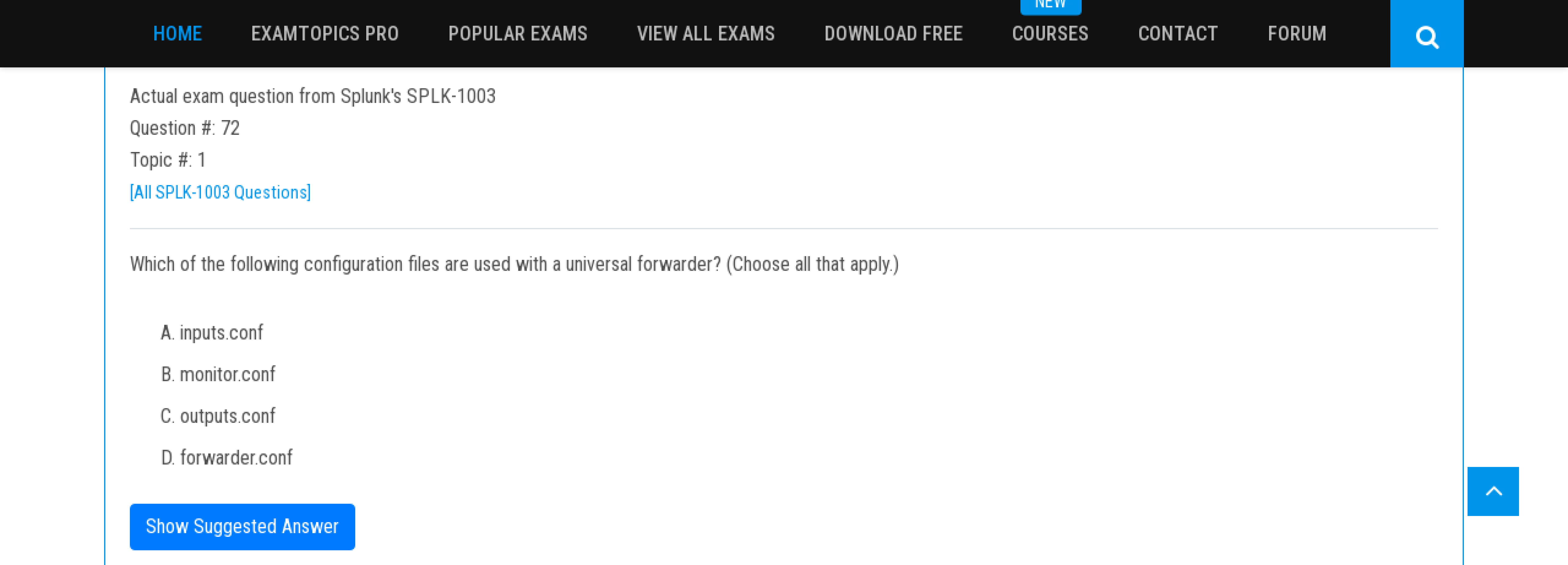
The volume of data from collecting log files from 50 Linux servers and 200 Windows servers will require multiple indexers. Following best practices, which types of Splunk component instances are needed?

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



Actual exam question from Splunk's SPLK-1003

Question #: 72

Topic #: 1

[All SPLK-1003 Questions]

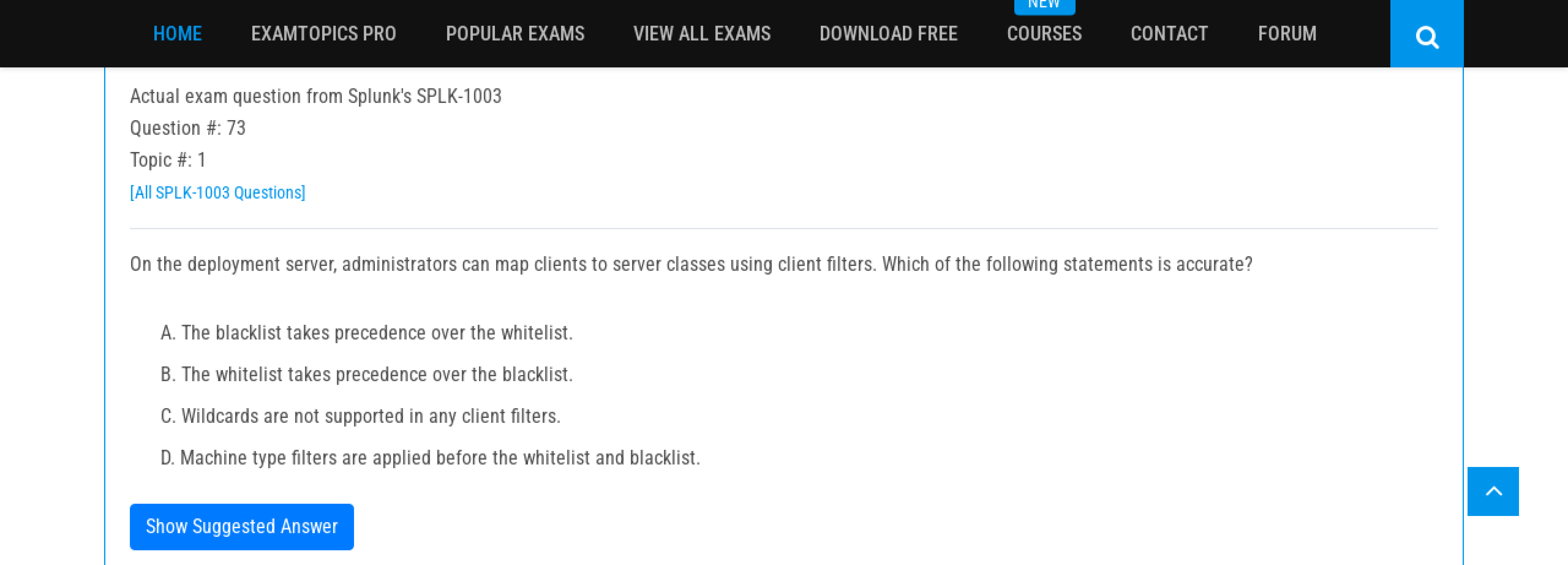
Which of the following configuration files are used with a universal forwarder? (Choose all that apply.)

A. inputs.conf

B. monitor.conf

C. outputs.conf

D. forwarder.conf



Actual exam question from Splunk's SPLK-1003

Question #: 73

Topic #: 1

[All SPLK-1003 Questions]

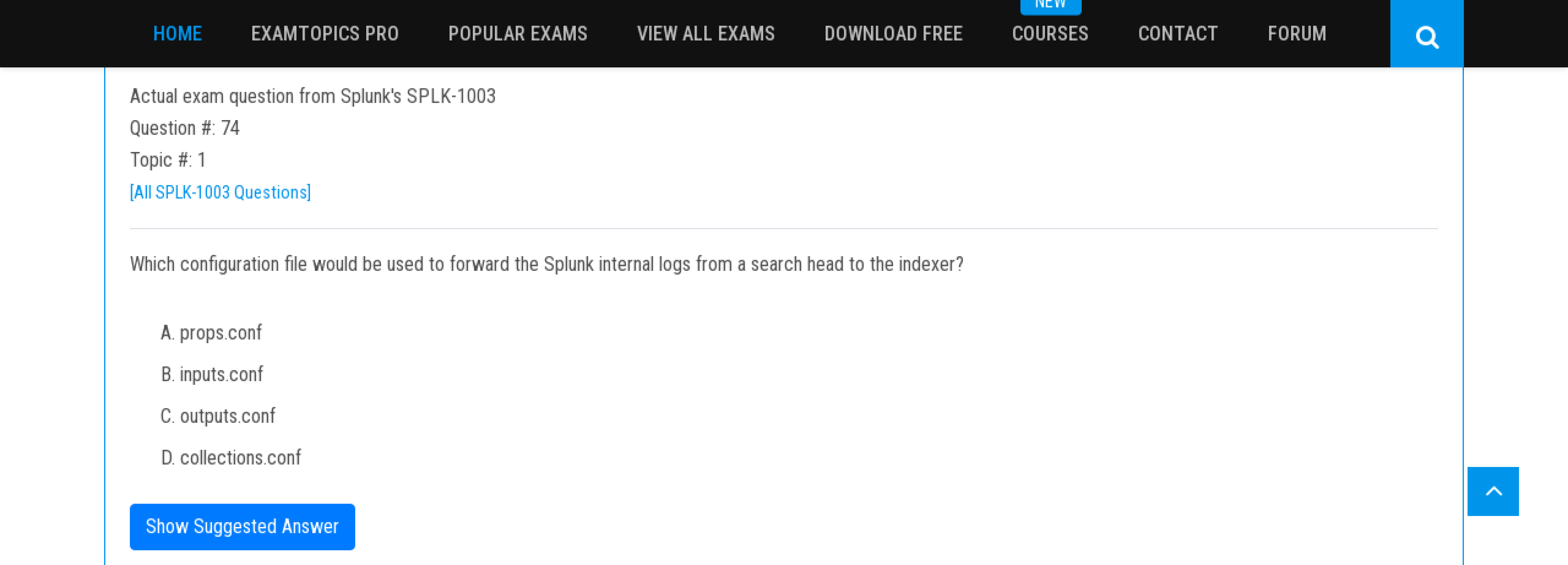
On the deployment server, administrators can map clients to server classes using client filters. Which of the following statements is accurate?

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.



Actual exam question from Splunk's SPLK-1003

Question #: 74

Topic #: 1

[All SPLK-1003 Questions]

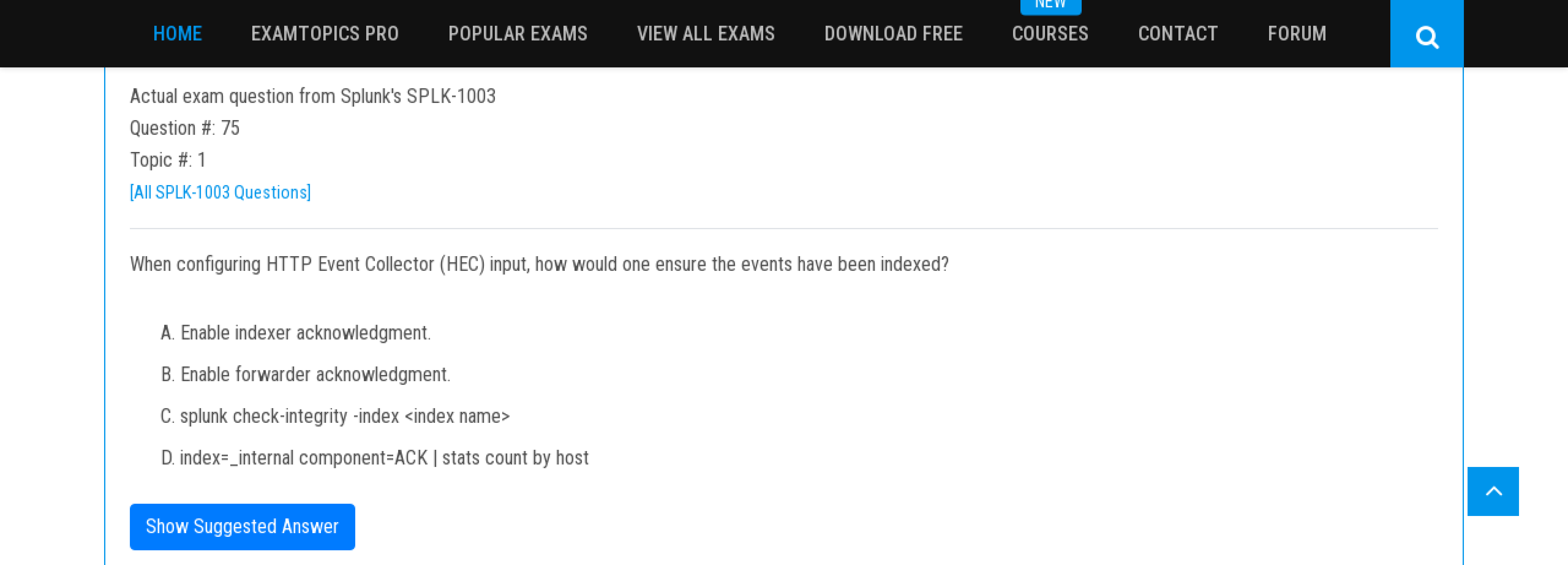
Which configuration file would be used to forward the Splunk internal logs from a search head to the indexer?

A. props.conf

B. inputs.conf

C. outputs.conf

D. collections.conf



Actual exam question from Splunk's SPLK-1003

Question #: 75

Topic #: 1

[All SPLK-1003 Questions]

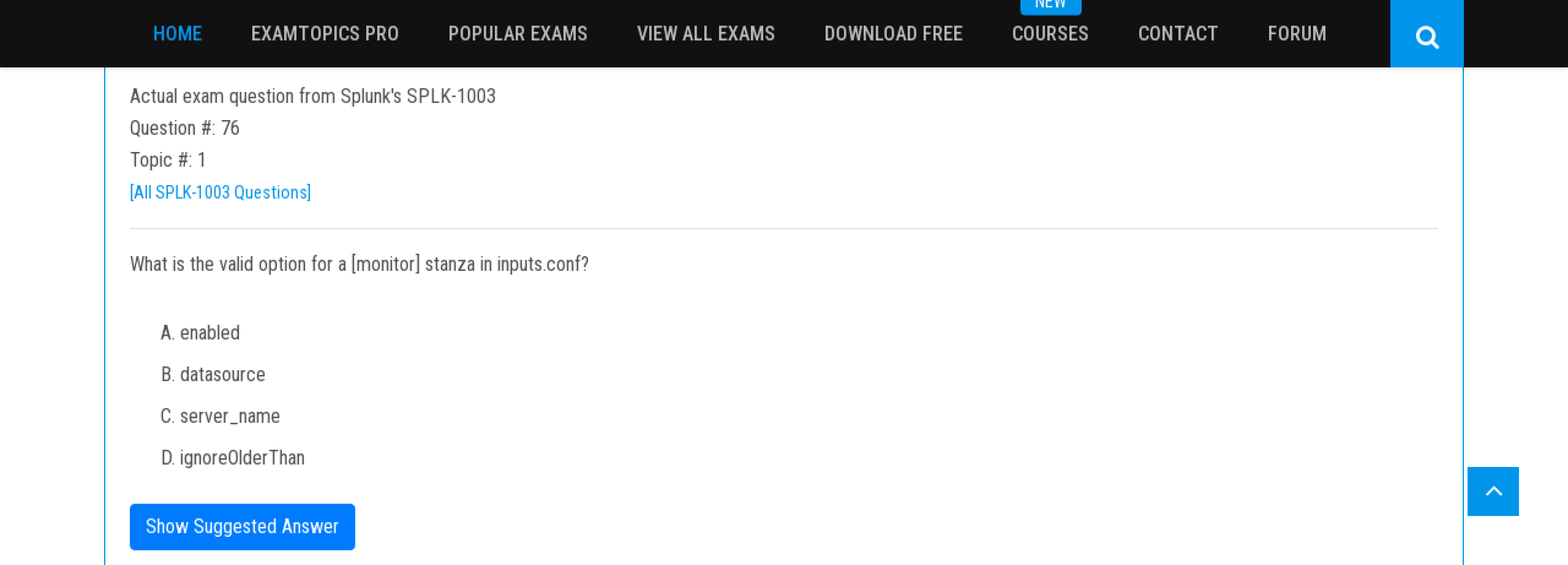
When configuring HTTP Event Collector (HEC) input, how would one ensure the events have been indexed?

A. Enable indexer acknowledgment.

B. Enable forwarder acknowledgment.

C. splunk check-integrity -index <index name>

D. index=_internal component=ACK | stats count by host



Actual exam question from Splunk's SPLK-1003

Question #: 76

Topic #: 1

[All SPLK-1003 Questions]

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

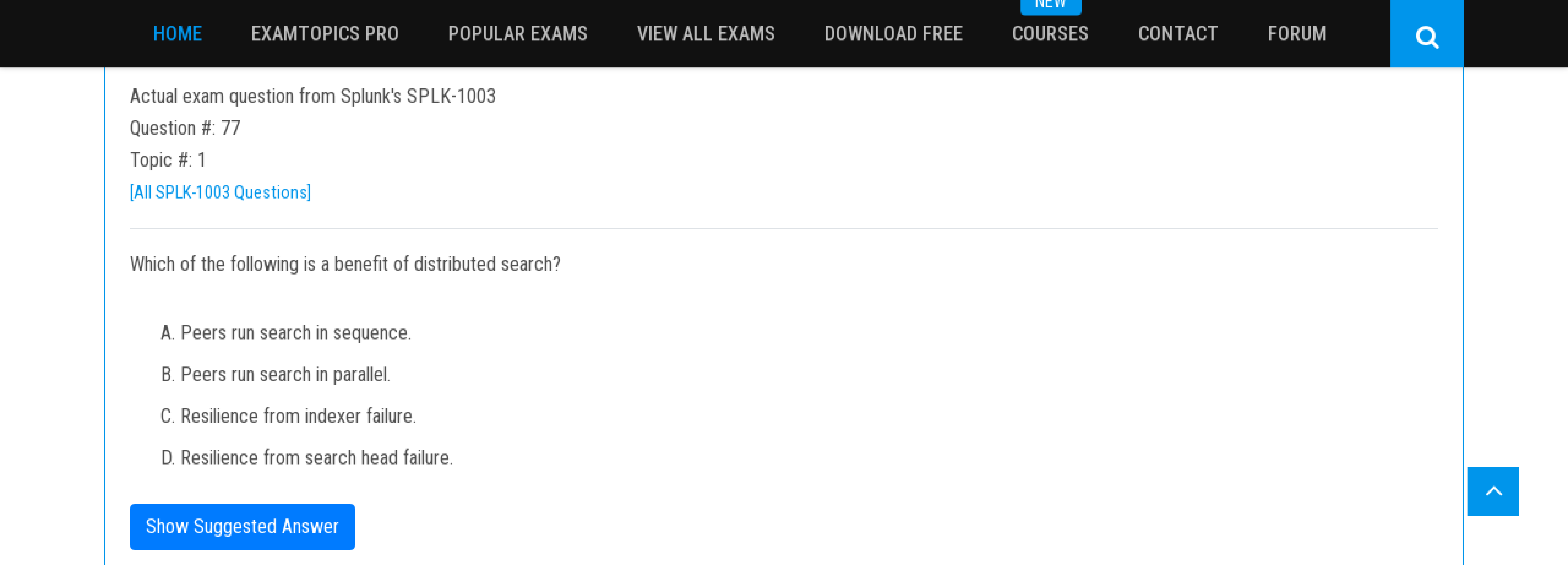
A. enabled

B. datasource

C. server_name

D. ignoreOlderThan

Show Suggested Answer



Actual exam question from Splunk's SPLK-1003

Question #: 77

Topic #: 1

[All SPLK-1003 Questions]

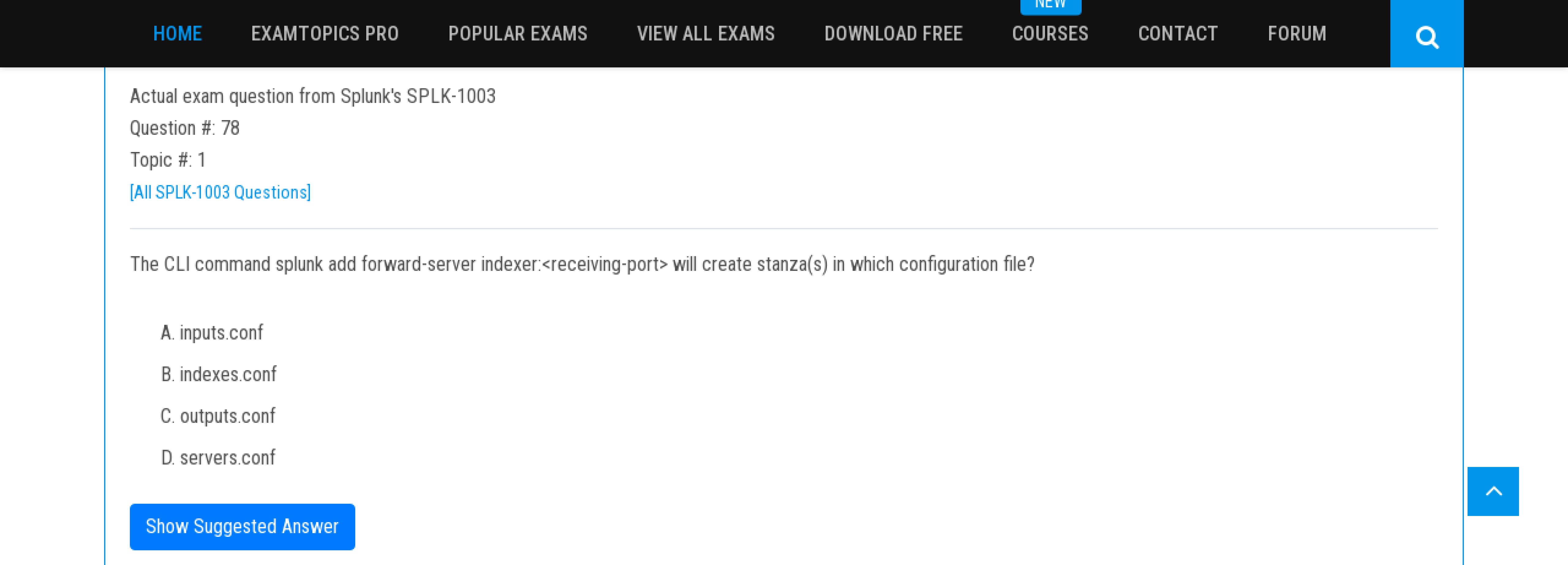
Which of the following is a benefit of distributed search?

A. Peers run search in sequence.

B. Peers run search in parallel.

C. Resilience from indexer failure.

D. Resilience from search head failure.



Actual exam question from Splunk's SPLK-1003

Question #: 78

Topic #: 1

[All SPLK-1003 Questions]

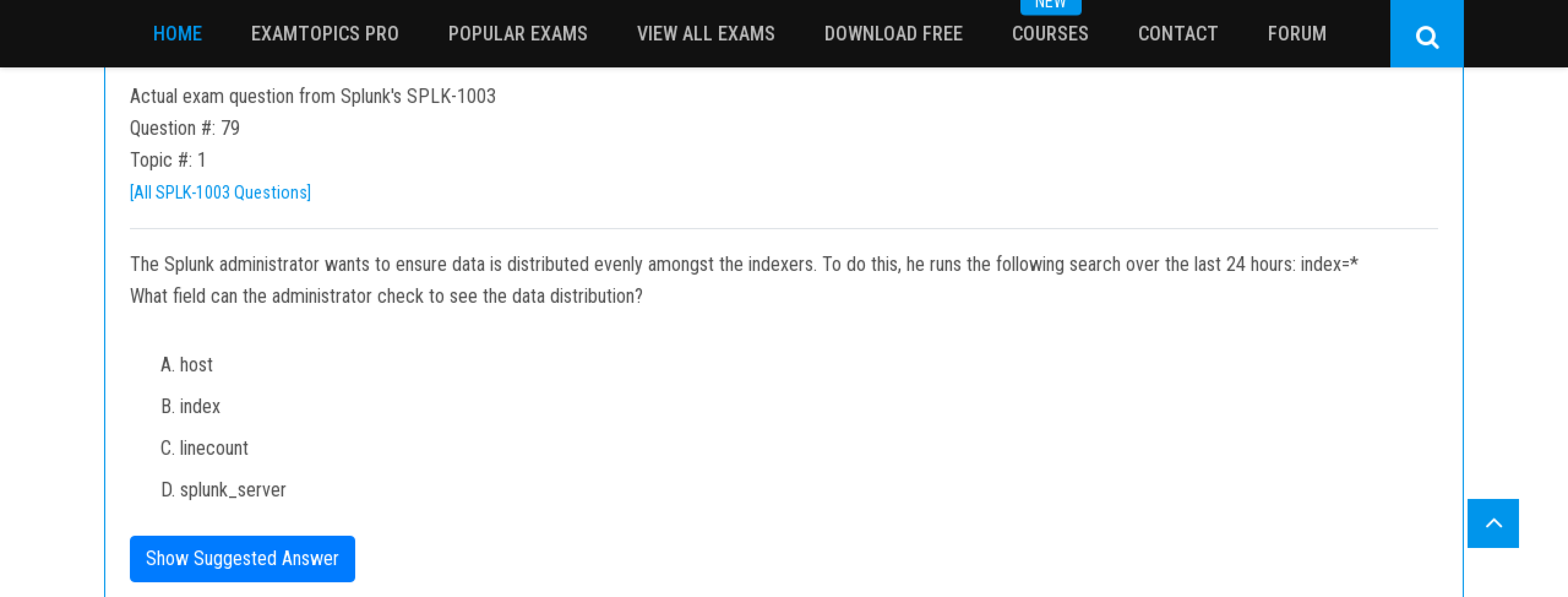
The CLI command splunk add forward-server indexer:<receiving-port> will create stanza(s) in which configuration file?

A. inputs.conf

B. indexes.conf

C. outputs.conf

D. servers.conf



Actual exam question from Splunk's SPLK-1003

Question #: 79

Topic #: 1

[All SPLK-1003 Questions]

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

Show Suggested Answer

Actual exam question from Splunk's SPLK-1003

Question #: 80

Topic #: 1

[All SPLK-1003 Questions]

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

Show Suggested Answer

Actual exam question from Splunk's SPLK-1003

Question #: 81

Topic #: 1

[All SPLK-1003 Questions]

Where are deployment server apps mapped to clients?

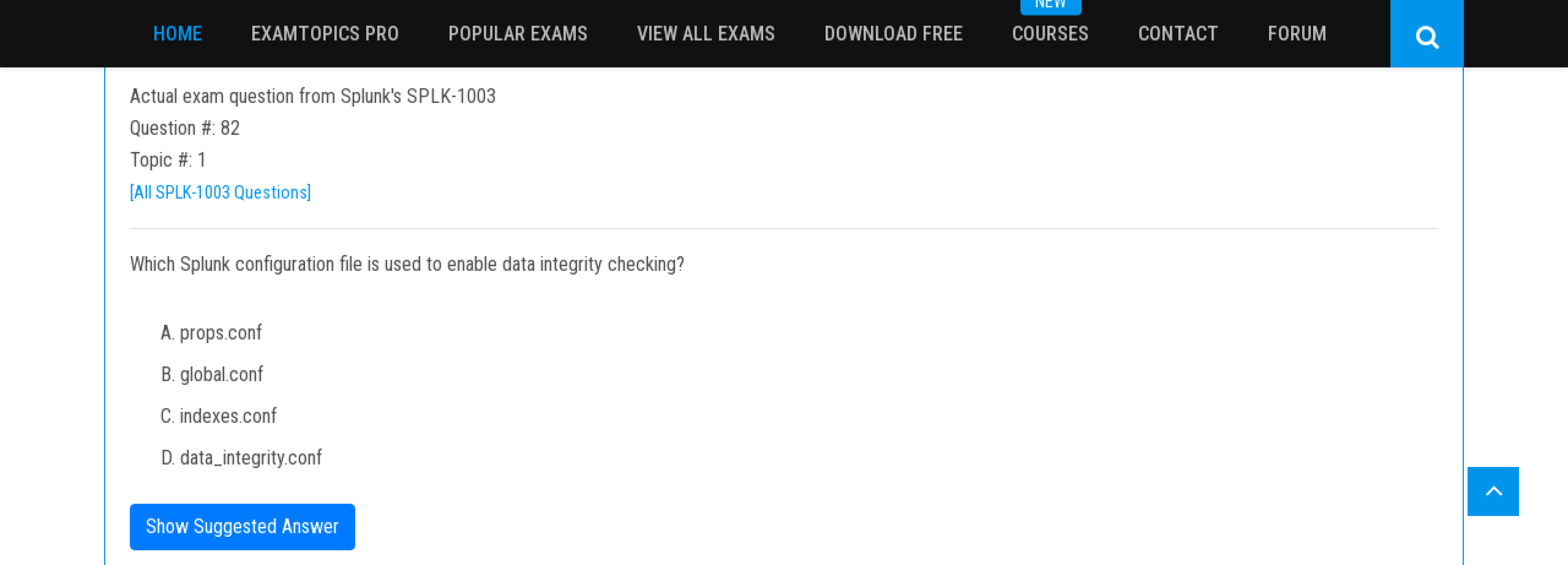
A. Apps tab in forwarder management interface or clientapps.conf.

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.

Show Suggested Answer



Actual exam question from Splunk's SPLK-1003

Question #: 82

Topic #: 1

[All SPLK-1003 Questions]

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

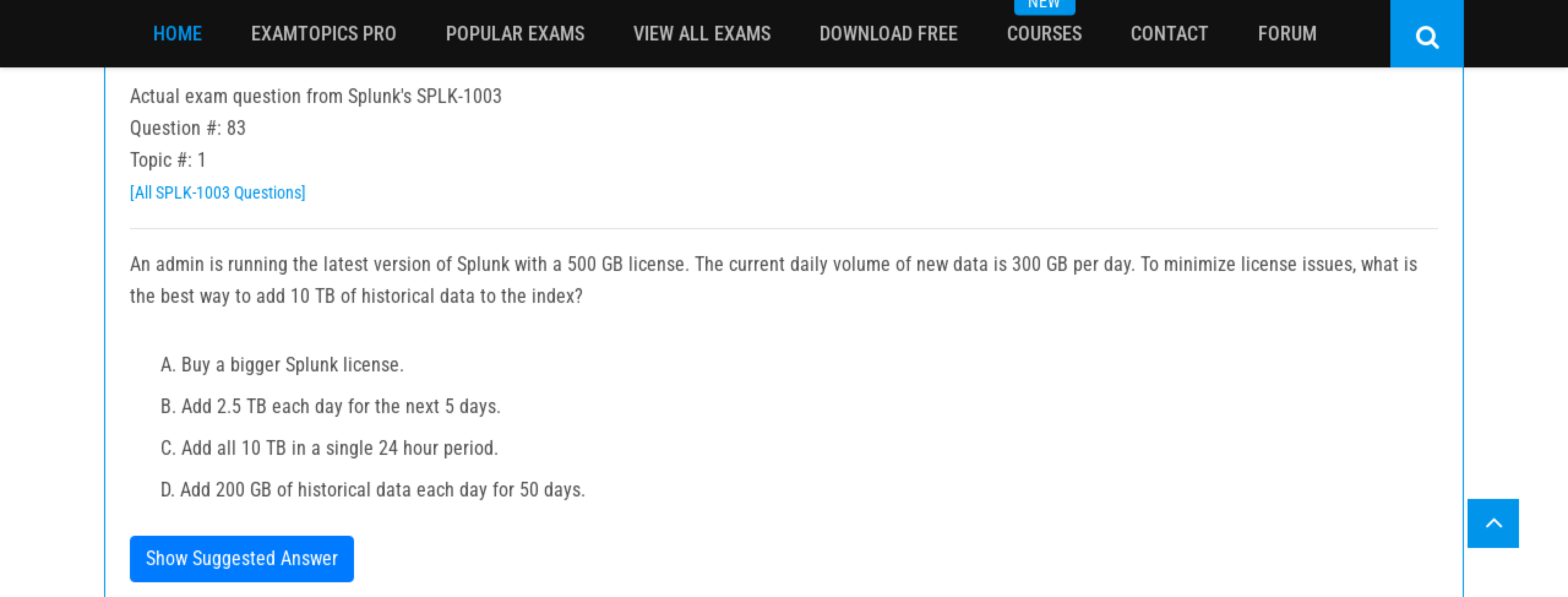
A. props.conf

B. global.conf

C. indexes.conf

D. data_integrity.conf

Show Suggested Answer



Actual exam question from Splunk's SPLK-1003
Question #: 83
Topic #: 1
[All SPLK-1003 Questions]

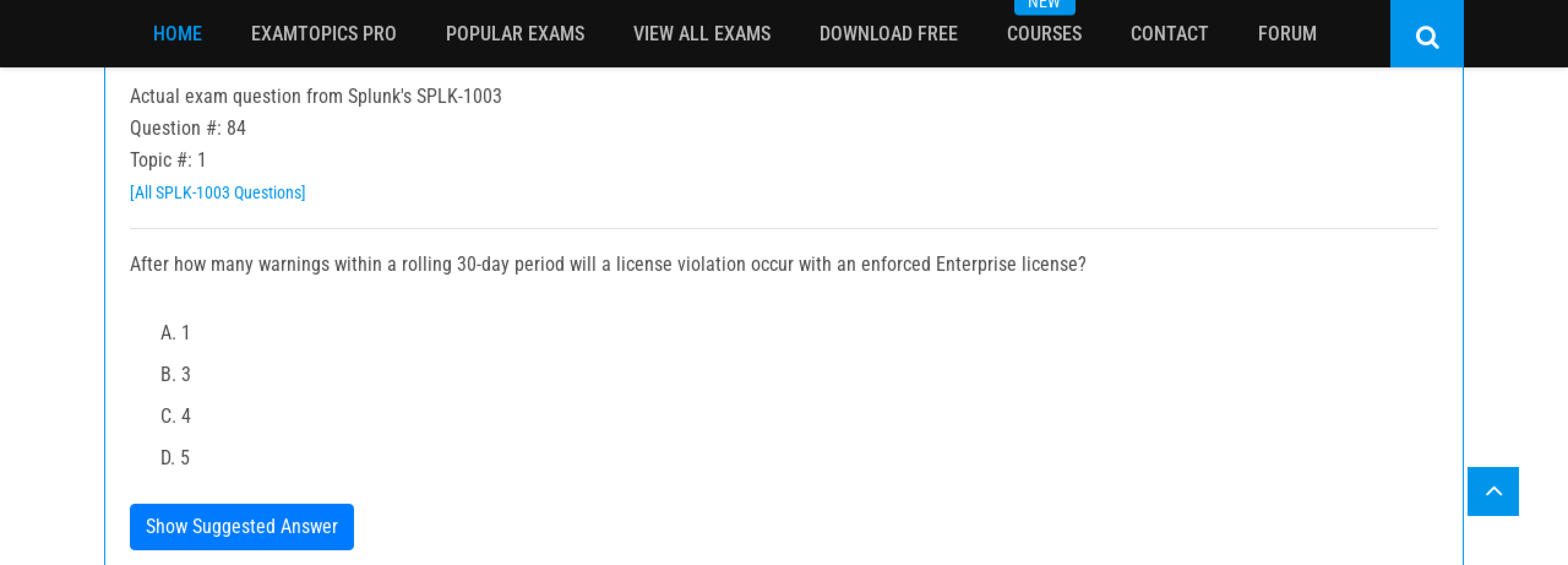
An admin is running the latest version of Splunk with a 500 GB license. The current daily volume of new data is 300 GB per day. To minimize license issues, what is the best way to add 10 TB of historical data to the index?

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.



Actual exam question from Splunk's SPLK-1003

Question #: 84

Topic #: 1

[All SPLK-1003 Questions]

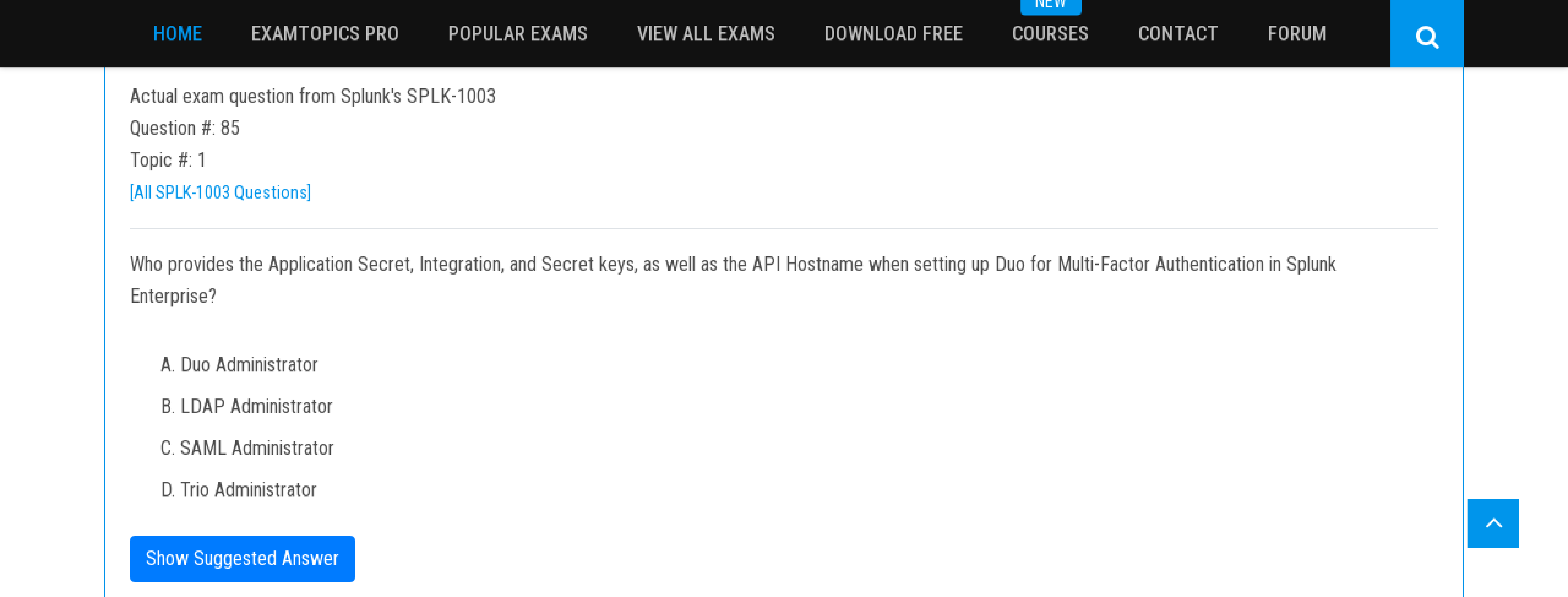
After how many warnings within a rolling 30-day period will a license violation occur with an enforced Enterprise license?

A. 1

B. 3

C. 4

D. 5



Actual exam question from Splunk's SPLK-1003

Question #: 85

Topic #: 1

[All SPLK-1003 Questions]

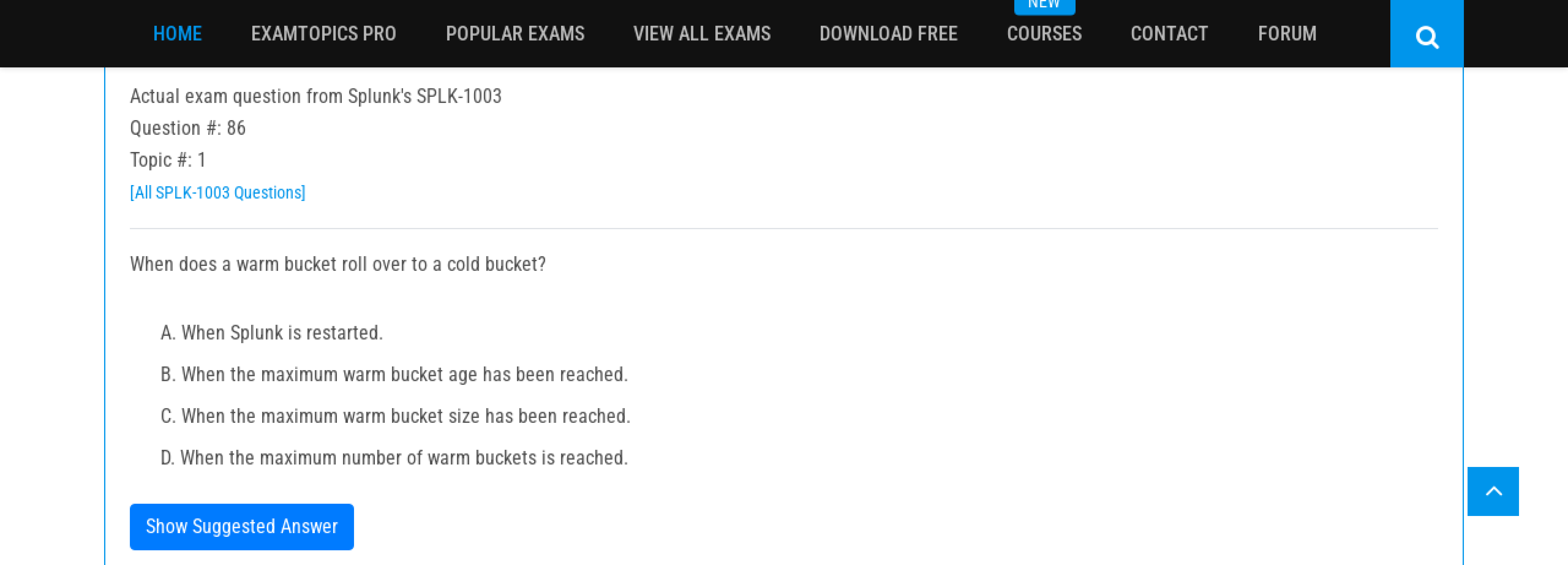
Who provides the Application Secret, Integration, and Secret keys, as well as the API Hostname when setting up Duo for Multi-Factor Authentication in Splunk Enterprise?

A. Duo Administrator

B. LDAP Administrator

C. SAML Administrator

D. Trio Administrator



Actual exam question from Splunk's SPLK-1003

Question #: 86

Topic #: 1

[All SPLK-1003 Questions]

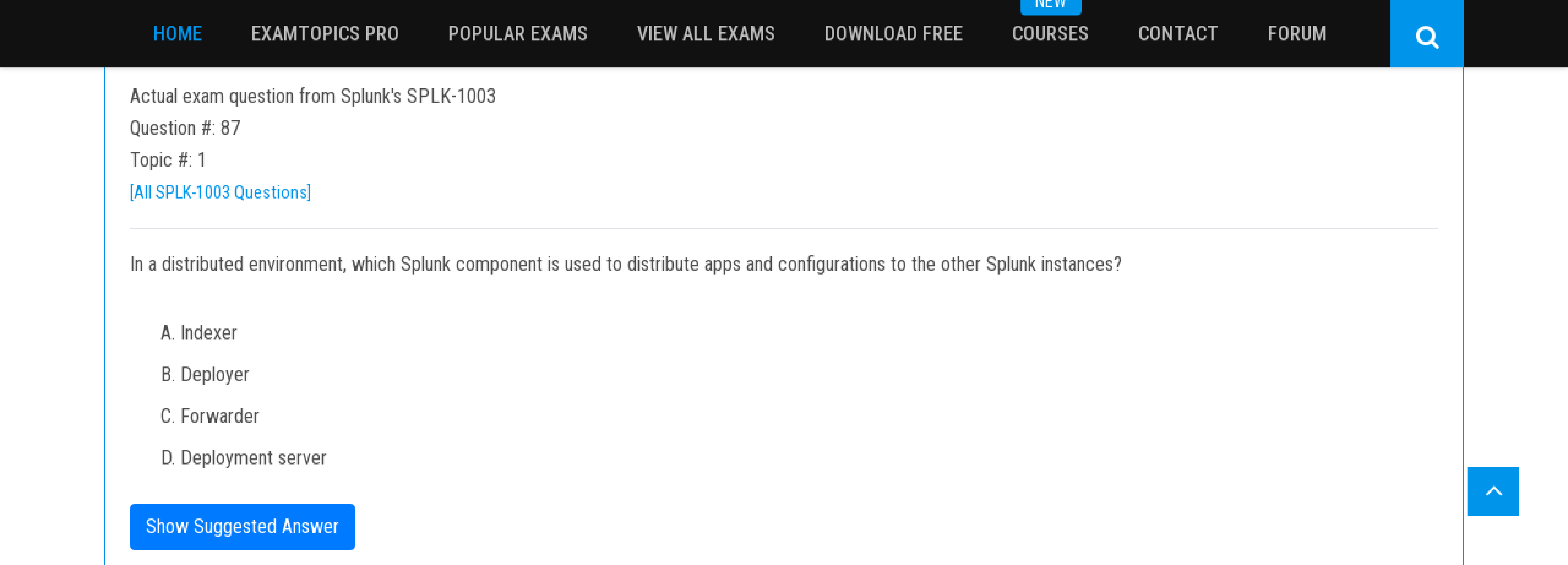
When does a warm bucket roll over to a cold bucket?

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.



Actual exam question from Splunk's SPLK-1003

Question #: 87

Topic #: 1

[All SPLK-1003 Questions]

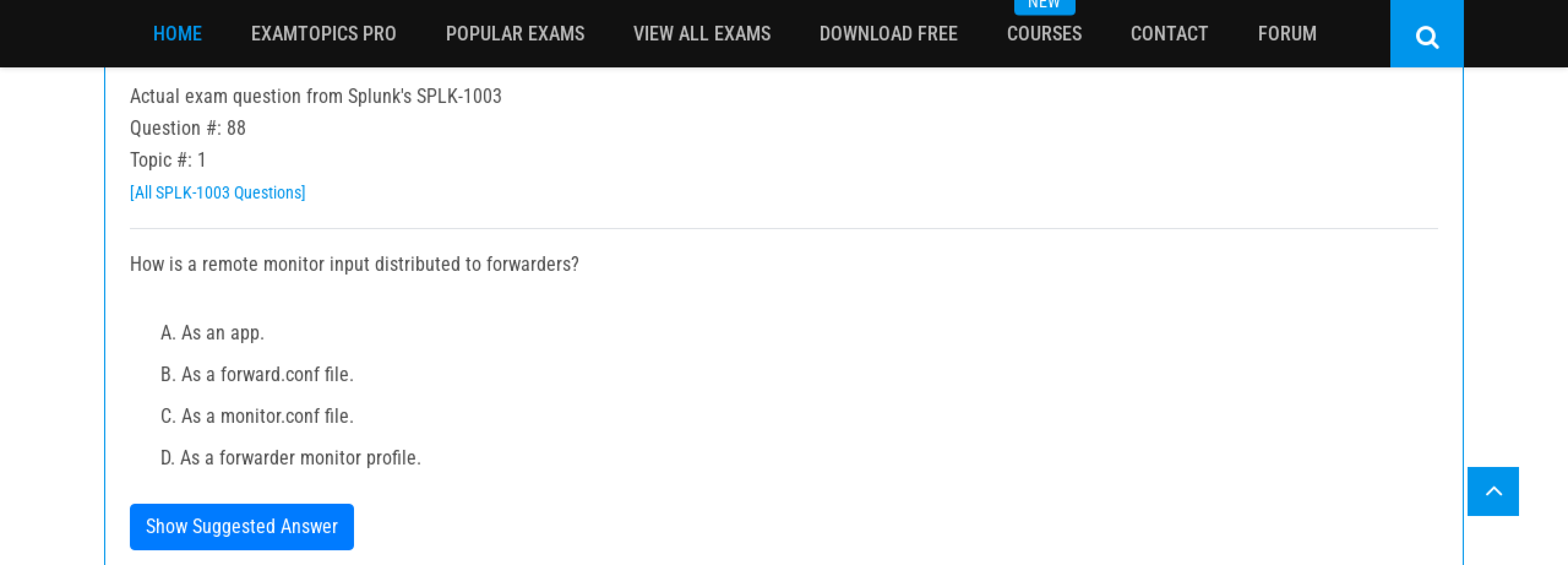
In a distributed environment, which Splunk component is used to distribute apps and configurations to the other Splunk instances?

A. Indexer

B. Deployer

C. Forwarder

D. Deployment server



Actual exam question from Splunk's SPLK-1003

Question #: 88

Topic #: 1

[All SPLK-1003 Questions]

How is a remote monitor input distributed to forwarders?

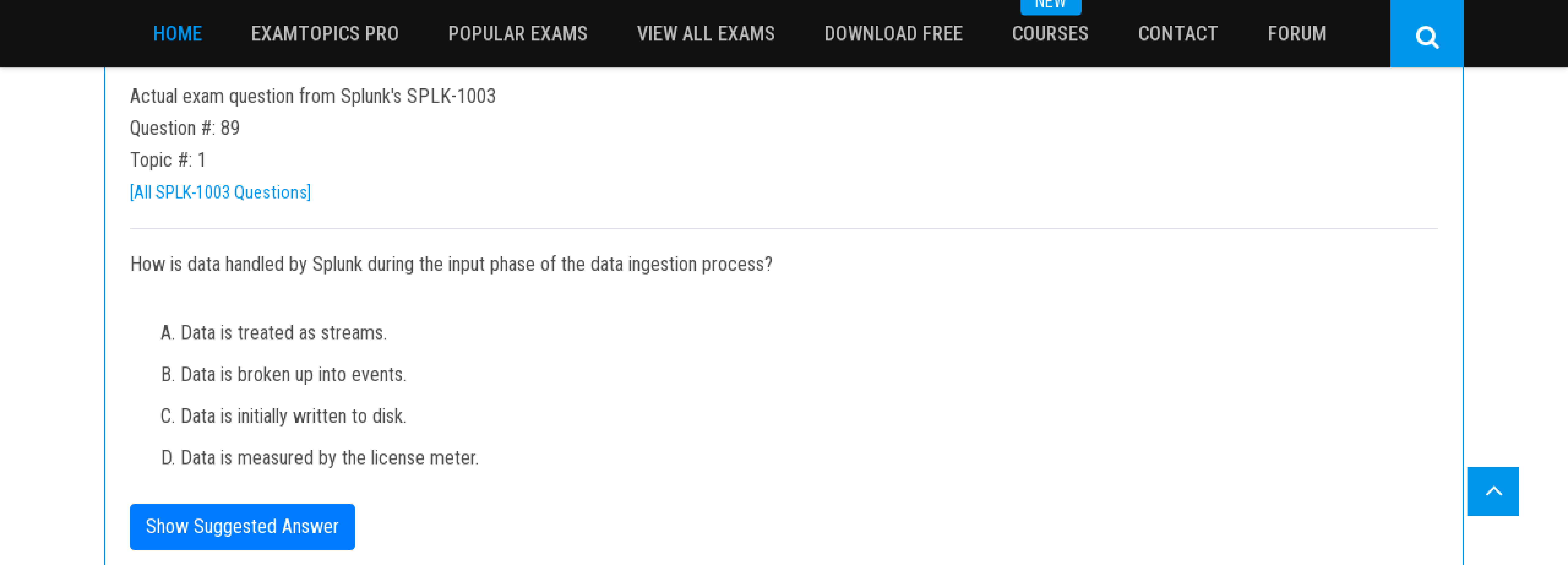
A. As an app.

B. As a forward.conf file.

C. As a monitor.conf file.

D. As a forwarder monitor profile.

Show Suggested Answer



Actual exam question from Splunk's SPLK-1003

Question #: 89

Topic #: 1

[All SPLK-1003 Questions]

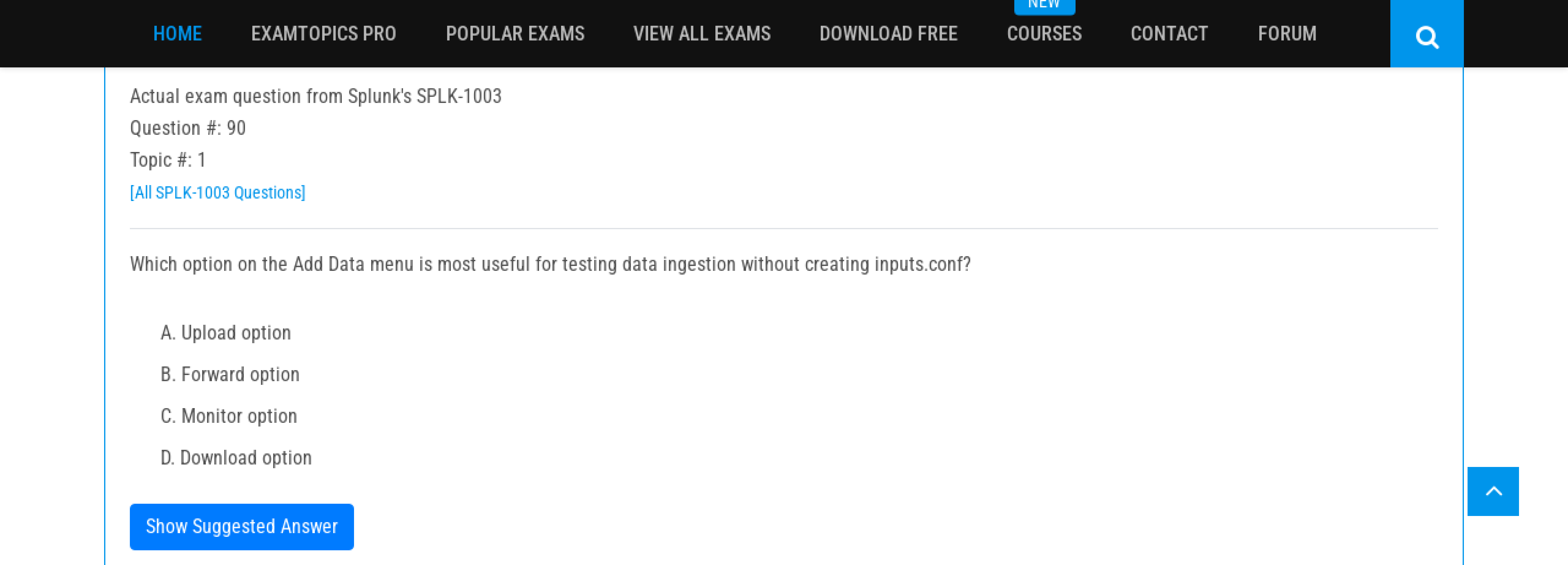
How is data handled by Splunk during the input phase of the data ingestion process?

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.



Actual exam question from Splunk's SPLK-1003

Question #: 90

Topic #: 1

[All SPLK-1003 Questions]

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

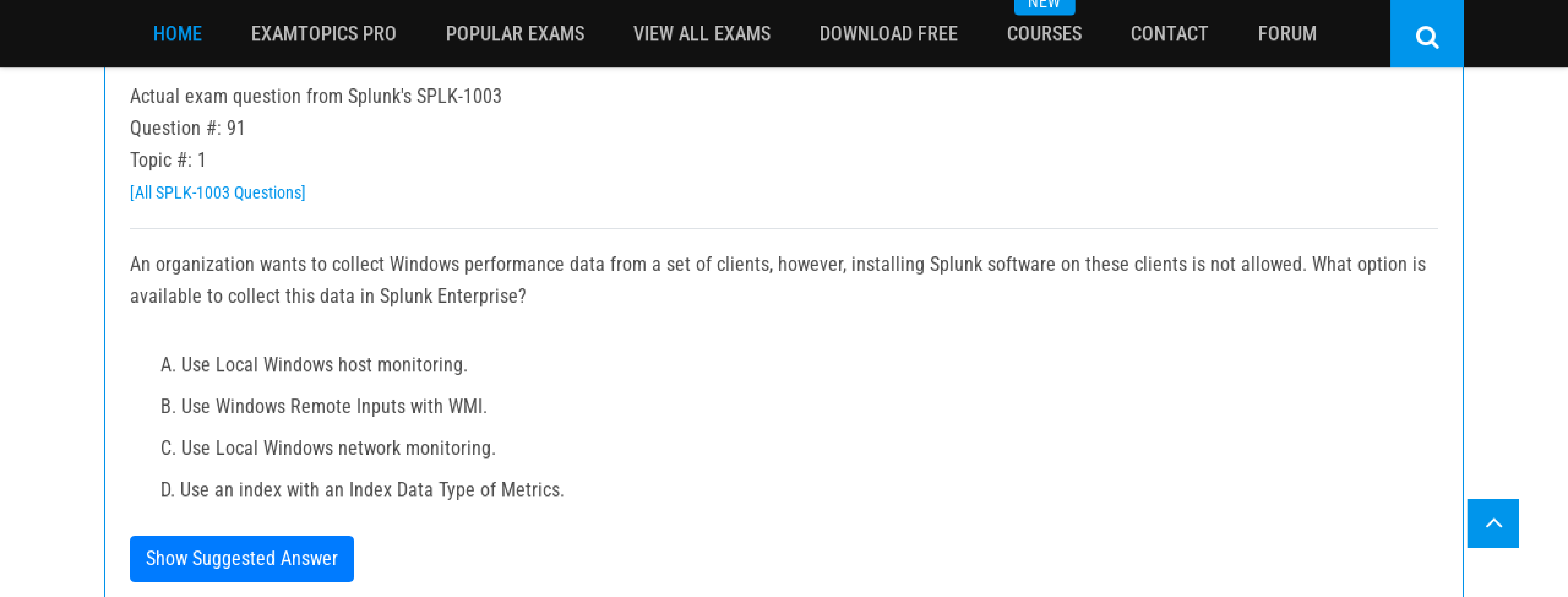
A. Upload option

B. Forward option

C. Monitor option

D. Download option

Show Suggested Answer



Actual exam question from Splunk's SPLK-1003

Question #: 91

Topic #: 1

[All SPLK-1003 Questions]

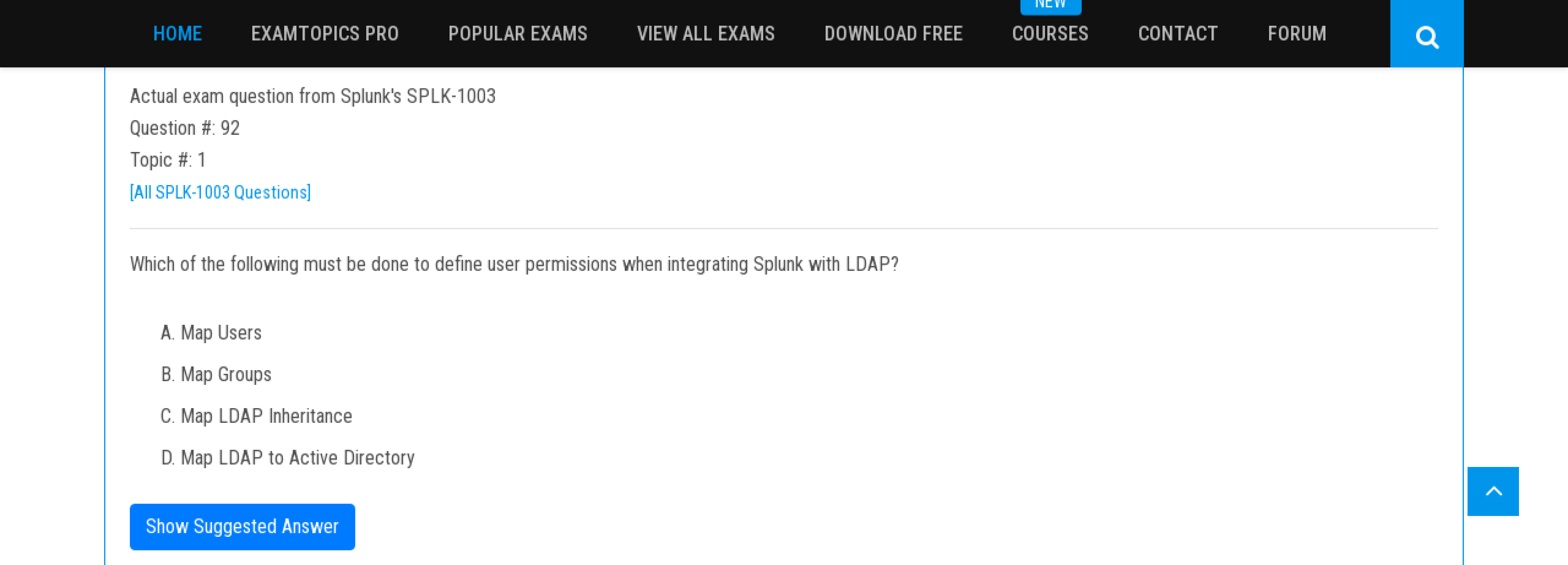
An organization wants to collect Windows performance data from a set of clients, however, installing Splunk software on these clients is not allowed. What option is available to collect this data in Splunk Enterprise?

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.



Actual exam question from Splunk's SPLK-1003

Question #: 92

Topic #: 1

[All SPLK-1003 Questions]

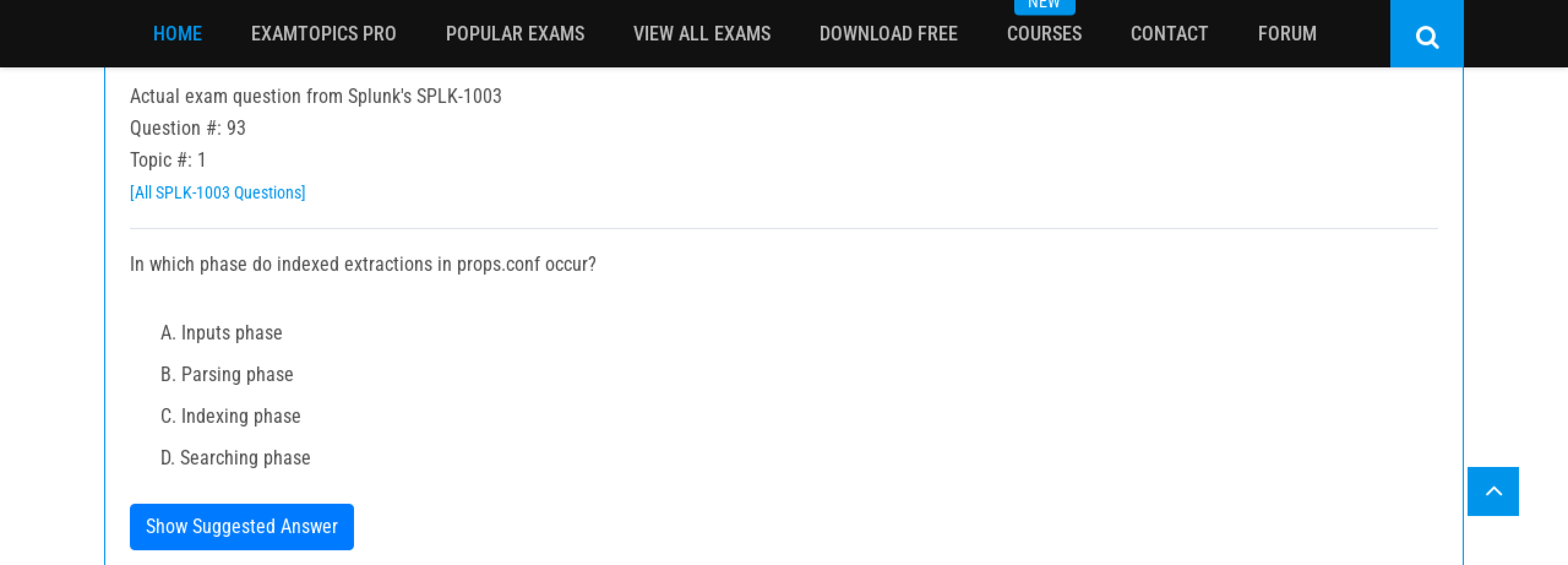
Which of the following must be done to define user permissions when integrating Splunk with LDAP?

A. Map Users

B. Map Groups

C. Map LDAP Inheritance

D. Map LDAP to Active Directory



Actual exam question from Splunk's SPLK-1003

Question #: 93

Topic #: 1

[All SPLK-1003 Questions]

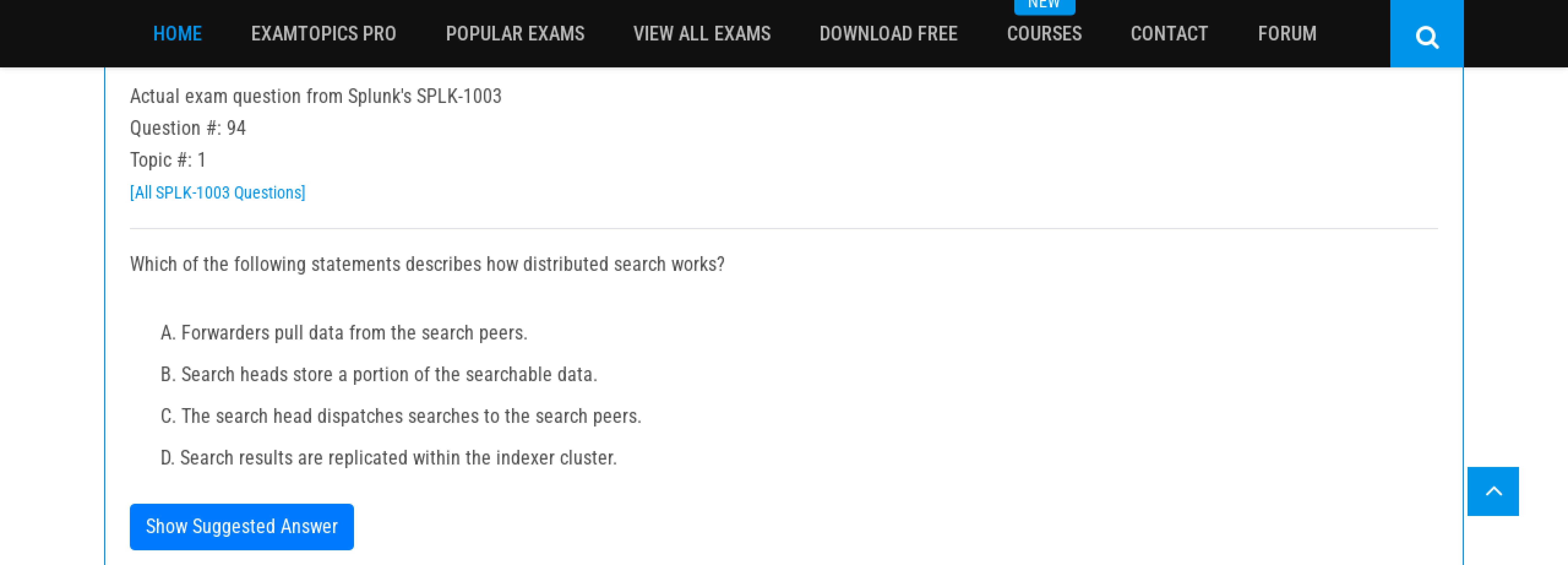
In which phase do indexed extractions in props.conf occur?

A. Inputs phase

B. Parsing phase

C. Indexing phase

D. Searching phase



Actual exam question from Splunk's SPLK-1003

Question #: 94

Topic #: 1

[All SPLK-1003 Questions]

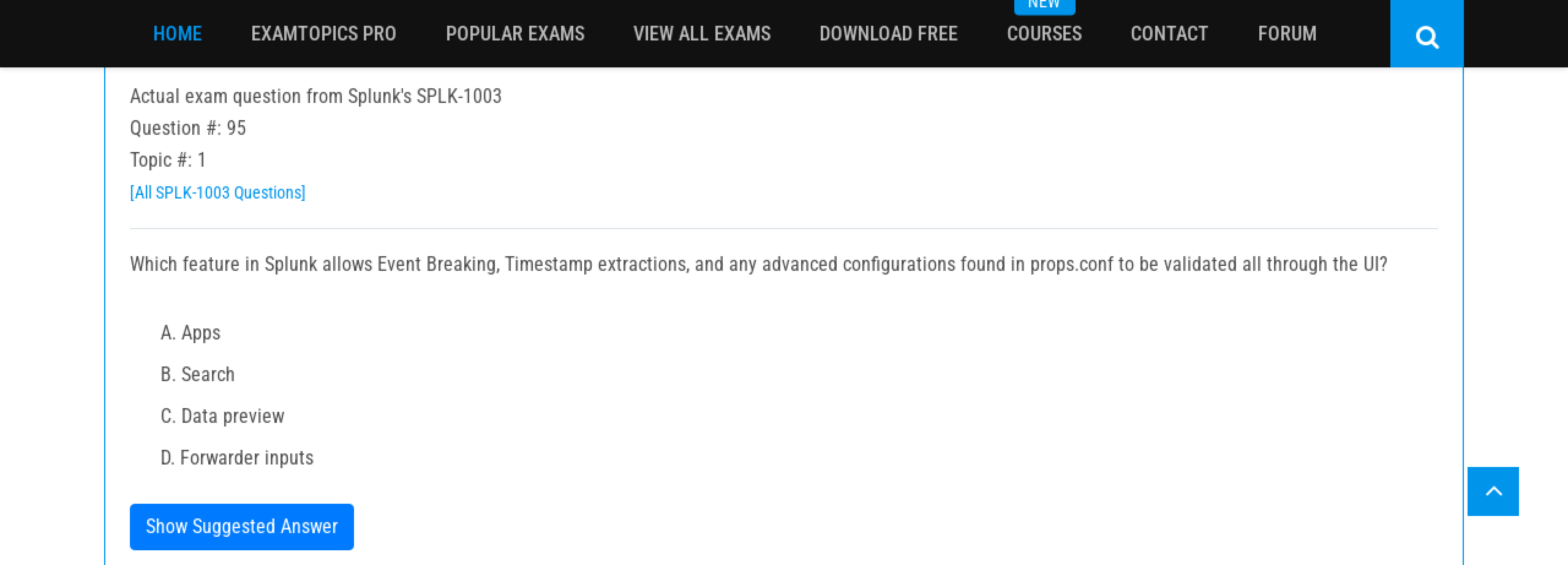
Which of the following statements describes how distributed search works?

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.



Actual exam question from Splunk's SPLK-1003

Question #: 95

Topic #: 1

[All SPLK-1003 Questions]

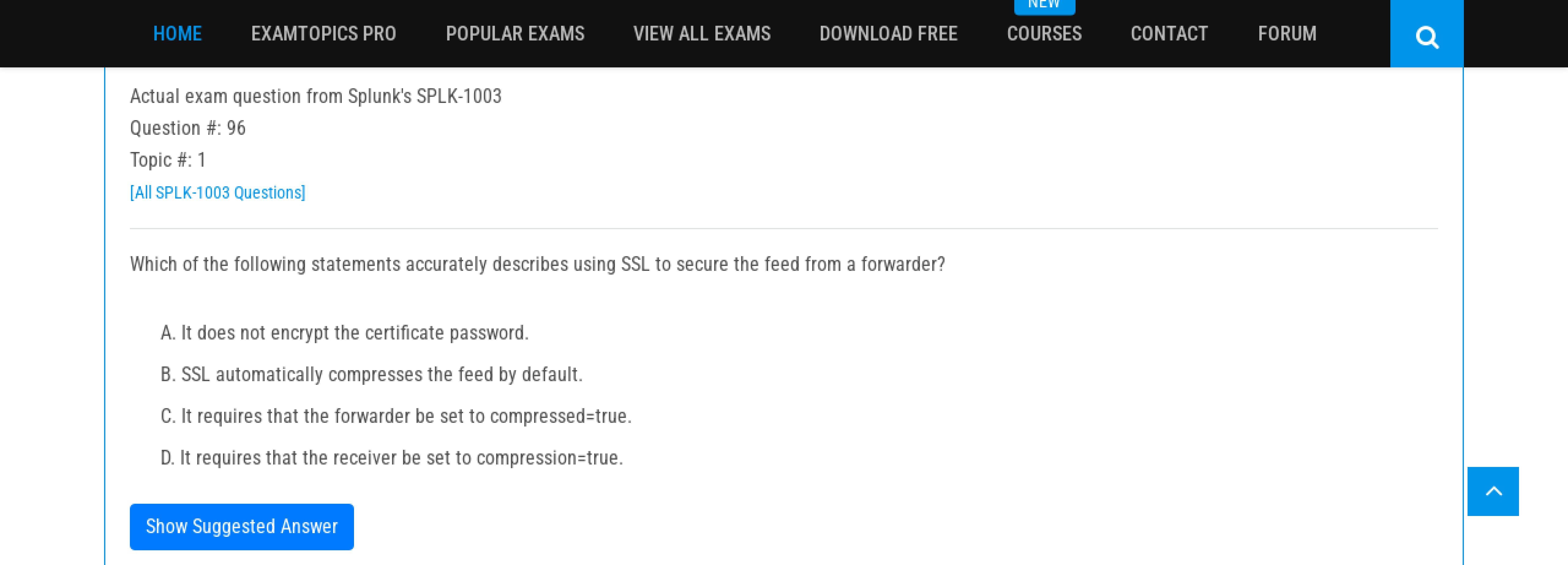
Which feature in Splunk allows Event Breaking, Timestamp extractions, and any advanced configurations found in props.conf to be validated all through the UI?

A. Apps

B. Search

C. Data preview

D. Forwarder inputs



Actual exam question from Splunk's SPLK-1003

Question #: 96

Topic #: 1

[All SPLK-1003 Questions]

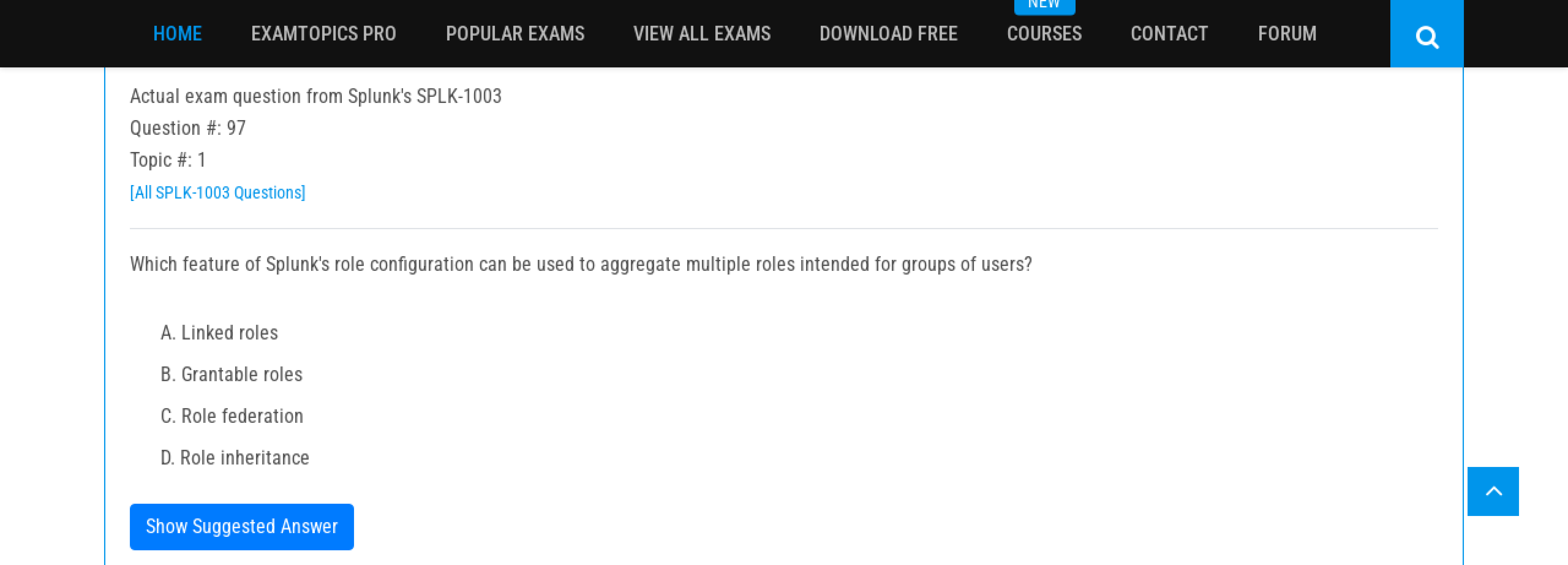
Which of the following statements accurately describes using SSL to secure the feed from a forwarder?

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.



Actual exam question from Splunk's SPLK-1003

Question #: 97

Topic #: 1

[All SPLK-1003 Questions]

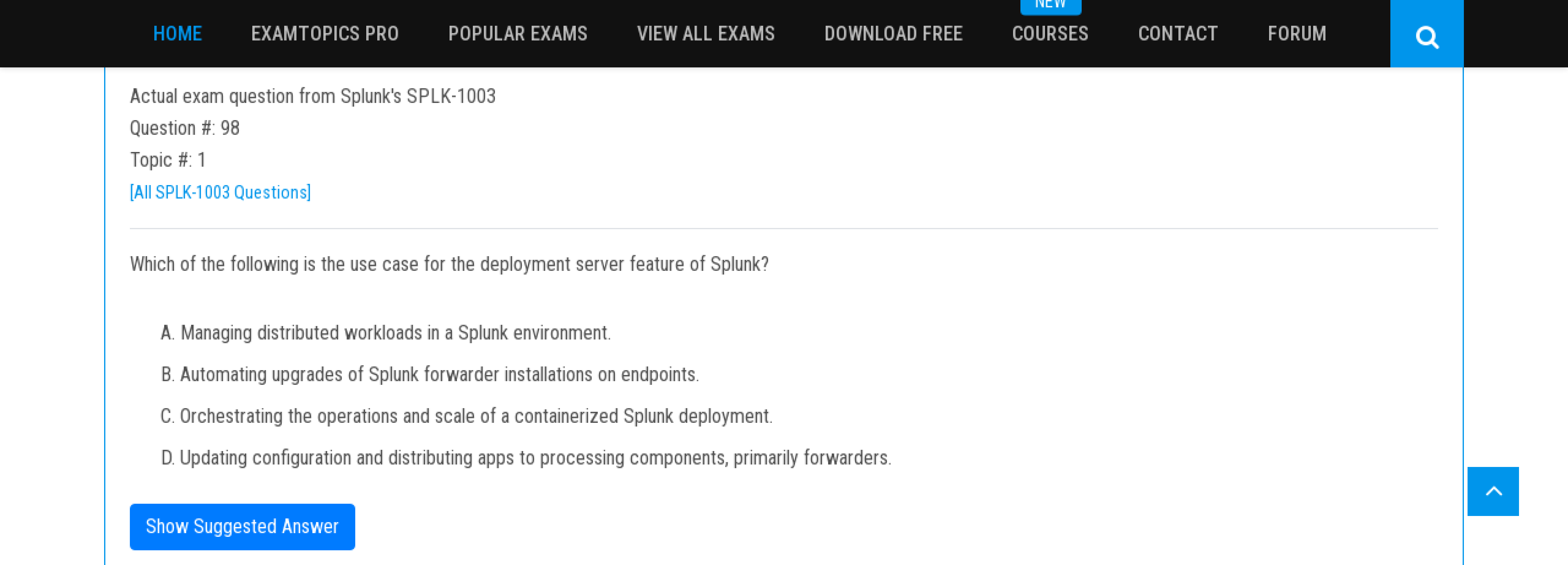
Which feature of Splunk's role configuration can be used to aggregate multiple roles intended for groups of users?

A. Linked roles

B. Grantable roles

C. Role federation

D. Role inheritance



Actual exam question from Splunk's SPLK-1003

Question #: 98

Topic #: 1

[All SPLK-1003 Questions]

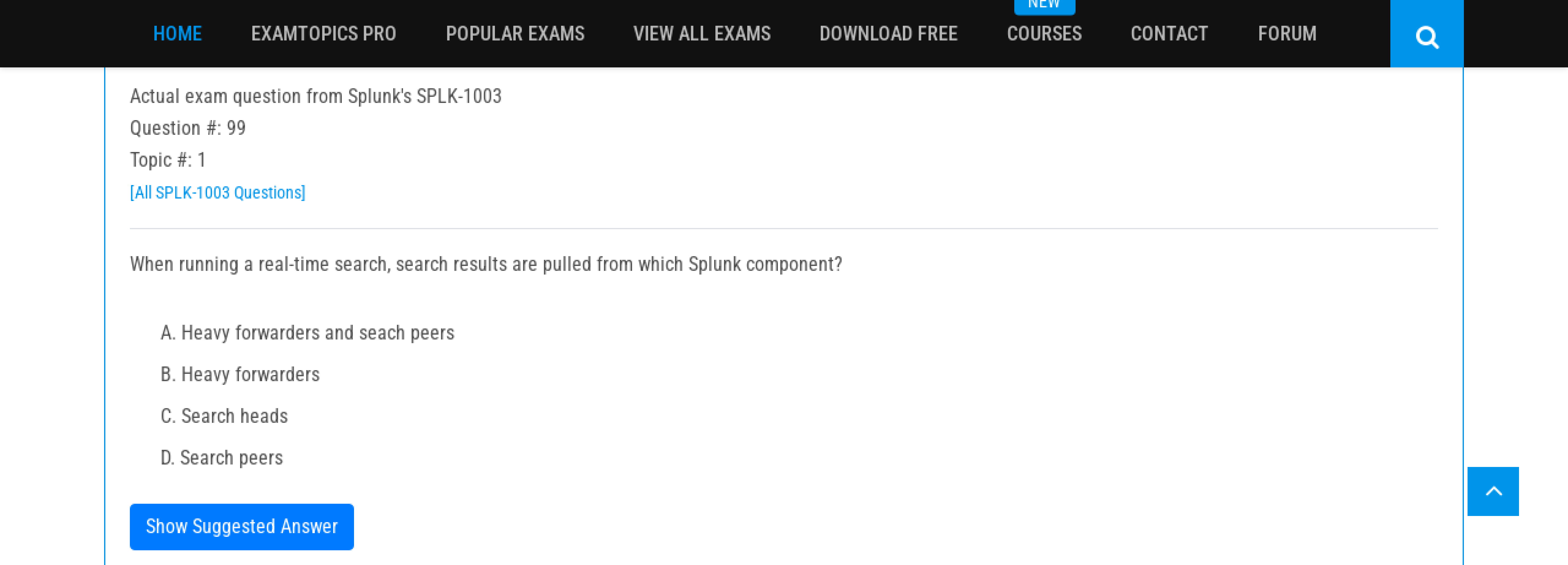
Which of the following is the use case for the deployment server feature of Splunk?

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.



Actual exam question from Splunk's SPLK-1003

Question #: 99

Topic #: 1

[All SPLK-1003 Questions]

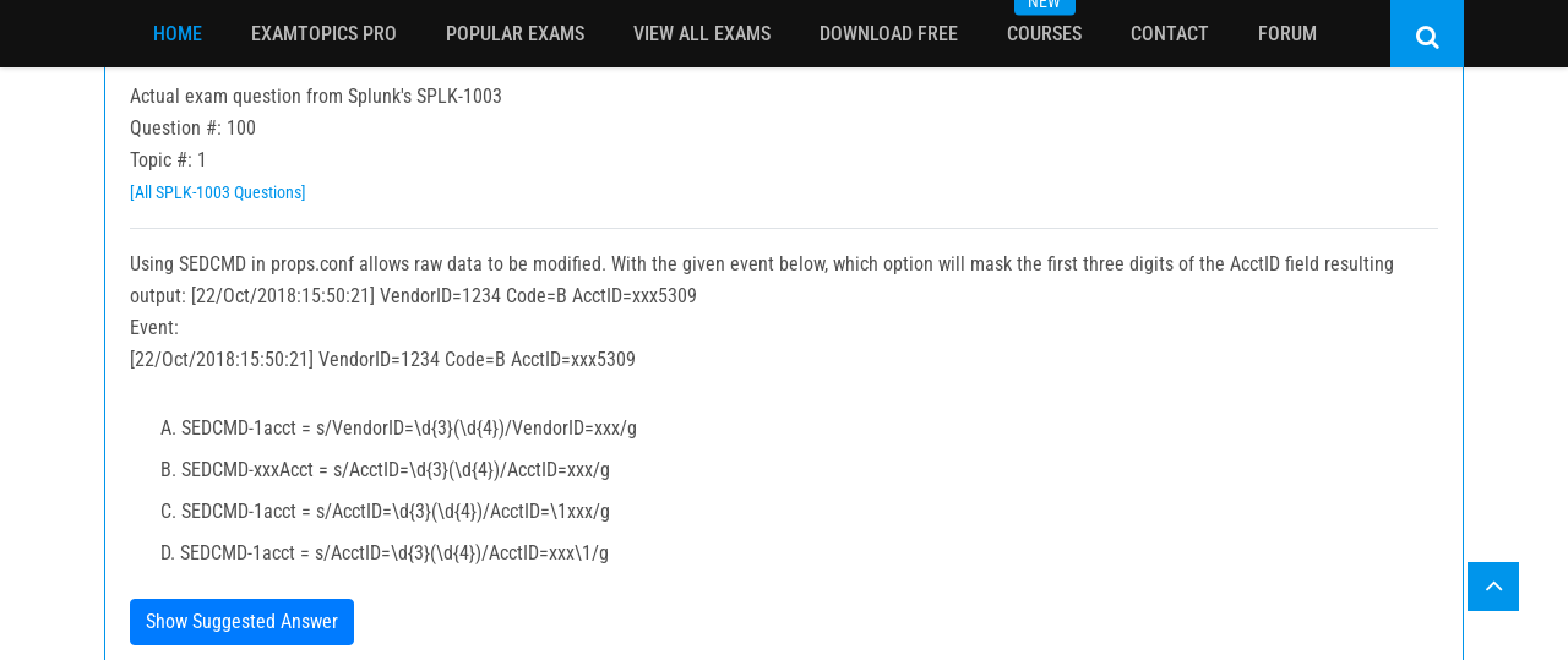
When running a real-time search, search results are pulled from which Splunk component?

A. Heavy forwarders and seach peers

B. Heavy forwarders

C. Search heads

D. Search peers



Actual exam question from Splunk's SPLK-1003

Question #: 100

Topic #: 1

[All SPLK-1003 Questions]

Using SEDCMD in props.conf allows raw data to be modified. With the given event below, which option will mask the first three digits of the AcctID field 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