Splunk.SPLK-1003.v2023-01-16.q120

Exam Code:	SPLK-1003
Exam Name:	Splunk Enterprise Certified Admin
Certification Provider:	Splunk
Free Question Number:	120
Version:	v2023-01-16
# of views:	3351
# of Questions views:	1200
https://www.freeqas.com/qa/Splunk/SPLK-1003/Splunk.SPLK-1003.v2023-01-16.q120.html	

NEW QUESTION: 1
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: 2
How do you remove missing forwarders from the Monitoring Console?
A. By rescanning active forwarders.
B. By rebuilding the forwarder asset table.
C. By reloading the deployment server.
D. By restarting Splunk.
Answer: B (LEAVE A REPLY)

NEW QUESTION: 3
In which Splunk configuration is the SEDCMDused?
A. props.conf
B. inputs.conf
C. indexes.conf
D. transforms.conf
Answer: (SHOW ANSWER)
Explanation
Explanation/Reference: https://answers.splunk.com/answers/212128/why-sedcmd-configured-in-propsconf-is-working- duri.html

NEW QUESTION: 4

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

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

B)

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

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

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

C)

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

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

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

D)

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

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

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

A. Option C

B. Option B

C. option A

D. Option D
Answer: (SHOW ANSWER)

NEW QUESTION: 5
When configuring monitor inputs with whitelists or blacklists, what is the supported method of filtering the lists?
A. Regular expression
B. Wildcard-only expression
C. Irregular expression
D. Slash notation
Answer: (SHOW ANSWER)

NEW QUESTION: 6
On the deployment server, administrators can map clients to server classes using client filters. Which of the following statements is accurate?
A. The blacklist takes precedence over the whitelist.
B. The whitelist takes precedence over the blacklist.
C. Wildcards are not supported in any client filters.
D. Machine type filters are applied before the whitelist and blacklist.
Answer: A (LEAVE A REPLY)
https://docs.splunk.com/Documentation/Splunk/8.2.1/Updating/Filterclients Reference:
same/td-p/390910

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

NEW QUESTION: 8
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: A (LEAVE A REPLY)
Explanation/Reference: https://docs.splunk.com/Documentation/Splunk/7.3.1/Data/UsetheHTTPEventCollector

NEW QUESTION: 9
If an update is made to an attribute in inputs.confon 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)
Explanation/Reference:
Reference https://community.splunk.com/t5/Archive/How-to-reindex-data-from-a-forwarder/td-p/93310

NEW QUESTION: 10
When running a real-time search, search results are pulled from which Splunk component?
A. Heavy forwarders and search peers
B. Heavy forwarders
C. Search heads
D. Search peers
Answer: D (LEAVE A REPLY)
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: 11
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
Answer: C (LEAVE A REPLY)
https://docs.splunk.com/Documentation/Splunk/8.1.1/DistSearch/Forwardsearchheaddata Per the provided Splunk reference URL by @hwangho, scroll to section Forward search head data, subsection titled, 2. Configure the search head as a forwarder. "Create an outputs.conf file on the search head that configures the search head for load-balanced forwarding across the set of search peers (indexers)."

NEW QUESTION: 12
Which Splunk indexer operating system platform is supported when sending logs from a Windows universal forwarder?
A. Linux platform only
B. None of the above.
C. Any OS platform
D. Windows platform only.
Answer: D (LEAVE A REPLY)

NEW QUESTION: 13
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.
Answer: D (LEAVE A REPLY)
"The search head replicates the knowledge bundle periodically in the background or when initiating a search. " "As part of the distributed search process, the search head replicates and distributes its knowledge objects to its search peers, or indexers. Knowledge objects include saved searches, event types, and other entities used in searching accorss indexes. The search head needs to distribute this material to its search peers so that they can properly execute queries on its behalf."

NEW QUESTION: 14
The priority of layered Splunk configuration files depends on the file's:
A. Owner
B. Weight
C. Context
D. Creation time
Answer: C (LEAVE A REPLY)
https://docs.splunk.com/Documentation/Splunk/7.3.0/Admin/Wheretofindtheconfigurationfiles
"To determine the order of directories for evaluating configuration file precedence, Splunk software considers each file's context. Configuration files operate in either a global context or in the context of the current app and user"

NEW QUESTION: 15
Which Splunk forwarder type allows parsing of data before forwarding to an indexer?
A. Universal forwarder
B. Advanced forwarder
C. Heavy forwarder
D. Parsing forwarder
Answer: C (LEAVE A REPLY)

NEW QUESTION: 16
Which of the following enables compression for universal forwarders in outputs. conf ?
A)

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

B)

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

C)

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

D)

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

A. Option C
B. Option B
C. Option D
D. Option A
Answer: B (LEAVE A REPLY)

NEW QUESTION: 17
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. _introspection
B. _checkpoint
C. _thefishbucket
D. _audit
Answer: D (LEAVE A REPLY)

NEW QUESTION: 18
In addition to single, non-clustered Splunk instances, what else can the deployment server push apps to?
A. Universal forwarders
B. Linux package managers
C. Splunk Cloud
D. Windows using WMI
Answer: (SHOW ANSWER)

NEW QUESTION: 19
Which setting allows the configuration of Splunk to allow events to span over more than one line?
A. SHOULD_LINEMERGE = false
B. BREAK_ONLY_BEFORE = <REGEX pattern>
C. SHOULD_LINEMERGE = true
D. BREAK_ONLY_BEFORE_DATE = true
Answer: (SHOW ANSWER)

NEW QUESTION: 20

Which forwarder type can parse data prior to forwarding?
A. Universal forwarder
B. Heaviest forwarder
C. Hyper forwarder
D. Heavy forwarder
Answer: (SHOW ANSWER)
Explanation/Reference: https://docs.splunk.com/Documentation/Splunk/7.3.1/Forwarding/Typesofforwarders

NEW QUESTION: 21
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: (SHOW ANSWER)
<https://docs.splunk.com/Documentation/Splunk/8.0.6/Updating/Deploymentserverarchitecture>
https://docs.splunk.com/Splexicon:Serverclass

NEW QUESTION: 22
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.
Answer: D (LEAVE A REPLY)
Explanation/Reference: https://docs.splunk.com/Documentation/Splunk/8.0.5/DistSearch/Whatsearchheadssend

NEW QUESTION: 23
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

NEW QUESTION: 24
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: A,D (LEAVE A REPLY)
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: 25
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. A verbose list of all configurations as they were when splunkd started.
B. list of all the configurations on-disk that Splunk contains.
C. A list of the current running props, conf configurations along with a file path from which the configuration was made
D. A list of props. conf configurations as they are on-disk along with a file path from which the configuration is located
Answer: (SHOW ANSWER)

NEW QUESTION: 26
Which Splunk component requires a Forwarder license?
A. Search head
B. Heavy forwarder
C. Heaviest forwarder
D. Universal forwarder
Answer: B (LEAVE A REPLY)
Explanation/Reference: https://answers.splunk.com/answers/70017/heavy-forwarder-costs-and-licenses.html

NEW QUESTION: 27
Within props. conf, which stanzas are valid for data modification? (select all that apply)
A. Source
B. Server
C. Sourcetype
D. Host
Answer: C (LEAVE A REPLY)

NEW QUESTION: 28
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: 29
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: D (LEAVE A REPLY)
Explanation/Reference:
https://docs.splunk.com/Documentation/Splunk/7.3.2/Installation/Systemrequirements#Supported_OSes

NEW QUESTION: 30
After configuring a universal forwarder to communicate with an indexer, which index can be checked via the Splunk Web UI for a successful connection?
index=main
A. index=test
B. index=summary
C. index=_internal
Answer: (SHOW ANSWER)
Explanation/Reference: https://docs.splunk.com/Documentation/Splunk/8.0.5/Security/Validateyourconfiguration

NEW QUESTION: 31
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.
Answer: (SHOW ANSWER)
https://docs.splunk.com/Documentation/Splunk/8.2.2/DistSearch/Whatisdistributedsearch Parallel reduce search processing If you struggle with extremely large high-cardinality searches, you might be able to apply parallel reduce processing to them to help them complete faster. You must have a distributed search environment to use parallel reduce search processing.

NEW QUESTION: 32
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
Answer: C (LEAVE A REPLY)
Reference:
Bypassautomaticsourcetypeassignment

NEW QUESTION: 33
In a distributed environment, which Splunk component is used to distribute apps and configurations to the other Splunk instances?
A. Deployment server
B. Forwarder
C. Indexer
D. Deployer
Answer: A (LEAVE A REPLY)

NEW QUESTION: 34
Which valid bucket types are searchable? (select all that apply)
A. Hot buckets
B. Cold buckets
C. Warm buckets
D. Frozen buckets
Answer: (SHOW ANSWER)
Hot/warm/cold/thawed bucket types are searchable. Frozen isn't searchable because its either deleted at that state or archived.

NEW QUESTION: 35

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 B

B. Option D

C. Option C

D. option A

Answer: D (LEAVE A REPLY)

NEW QUESTION: 36

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.

Answer: A (LEAVE A REPLY)

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

NEW QUESTION: 37

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

Answer: A (LEAVE A REPLY)

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

NEW QUESTION: 38
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
Answer: A,B (LEAVE A REPLY)
Explanation
Explanation/Reference:
https://docs.splunk.com/Documentation/Forwarder/7.3.1/Forwarder/HowtoforwarddatatoSplunkEnterprise#Define_inputs_on_the_universal_forwarder_with_configuration_files

NEW QUESTION: 39
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]
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
B. [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
C. [distributedSearch:NYC]
default = false
servers = nyc1:8089, nyc2:8089
[distributedSearch:HOUSTON]
default = false
servers = houston1:8089, houston2:8089
D. [distributedSearch]
servers =nyc1, nyc2, houston1, houston2
[distributedSearch:NYC]
default = false

servers = nyc1, nyc2
[distributedSearch:HOUSTON]
default = false
servers = houston1, houston2
Answer: A (LEAVE A REPLY)

NEW QUESTION: 40
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=_internal
B. index=test
C. index=main
D. index=summary
Answer: A (LEAVE A REPLY)

NEW QUESTION: 41
In which phase do indexed extractions in props.conf occur?
A. Indexing phase
B. Inputs phase
C. Searching phase
D. Parsing phase
Answer: (SHOW ANSWER)

NEW QUESTION: 42
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. Forwarder inputs
D. Apps
Answer: (SHOW ANSWER)

NEW QUESTION: 43
What action is required to enable forwarder management in Splunk Web?
A. Navigate to Settings > Server Settings > General Settings, and set an App server port.
B. Navigate to Settings > Forwarding and receiving, and click on Enable Forwarding.
C. Create a server class and map it to a client in SPLUNK_HOME/etc/system/local/serverclass.conf.
D. Place an app in the SPLUNK_HOME/etc/deployment-apps directory of the deployment server.
Answer: (SHOW ANSWER)
Reference:
https://docs.splunk.com/Documentation/MSApp/2.0.3/MSInfra/Setupadeploymentserver
"To activate deployment server, you must place at least one app into %SPLUNK_HOME%\etc\deployment-apps on the host you want to act as deployment server. In this case, the app is the "send to indexer" app you created earlier, and the host is the indexer you set up initially.

NEW QUESTION: 44

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: 45

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: C (LEAVE A REPLY)

Explanation/Reference: https://docs.splunk.com/Documentation/SplunkCloud/8.0.2006/Data/ Bypassautomaticsourcetypeassignment

NEW QUESTION: 46

Which Splunk component performs indexing and responds to search requests from the search head?

A. Forwarder

B. Search head cluster

C. Search peer

D. License master

Answer: (SHOW ANSWER)

NEW QUESTION: 47
What are the required stanza attributes when configuring the transforms. conf to manipulate or remove events?
A. REGEX, DEST_KEY FORMATTING
B. REGEX. SRC_KEY, FORMAT
C. REGEX, DEST_KEY, FORMAT
D. REGEX, DEST. FORMAT
Answer: (SHOW ANSWER)

NEW QUESTION: 48
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. transforms.conf
[mask-SSN]
REGEX = (?ms)^(.)\<[SSN>\d{3}-?\d{2}-?(\d{4}.*)$"
FORMAT = $1<SSN>###-##-$2
DEST_KEY = _raw
B. props.conf
[mask-SSN]
REGEX = (?ms)^(.)\<[SSN>\d{3}-?\d{2}-?(\d{4}.*)$"
FORMAT = $1<SSN>###-##-$2
DEST_KEY = _raw
C. transforms.conf
[mask-SSN]
REX = (?ms)^(.)\<[SSN>\d{3}-?\d{2}-?(\d{4}.*)$"
FORMAT = $1<SSN>###-##-$2
DEST_KEY = _raw
D. props.conf
[mask-SSN]
REX = (?ms)^(.)\<[SSN>\d{3}-?\d{2}-?(\d{4}.*)$"
FORMAT = $1<SSN>###-##-$2
KEY = _raw
Answer: B (LEAVE A REPLY)

NEW QUESTION: 49

Which Splunk component does a search head primarily communicate with?
A. Cluster master
B. Deployment server
C. Forwarder
D. Indexer
Answer: (SHOW ANSWER)

NEW QUESTION: 50
Where can scripts for scripted inputs reside on the host file system? (select all that apply)
A. $SFLUNK_HOME/bin/scripts
B. $SPLUNK_HOME/etc/apps/bin
C. $SPLUNK_HOME/etc/system/bin
D. $S?LUNK_HOME/etc/apps/<your_app>/bin_
Answer: A,C,D (LEAVE A REPLY)
"Where to place the scripts for scripted inputs. The script that you refer to in $SCRIPT can reside in only one of the following places on the host file system:
$SPLUNK_HOME/etc/system/bin
$SPLUNK_HOME/etc/apps/<your_App>/bin
$SPLUNK_HOME/bin/scripts
As a best practice, put your script in the bin/ directory that is nearest to the inputs.conf file that calls your script on the host file system."

NEW QUESTION: 51
Which parent directory contains the configuration files in Splunk?
A. SSFLUNK_HOME/etc
B. SSPLUNK_HOME/var
C. SSPLUNK_HOME/conf
D. SSPLUNK_HOME/default
Answer: A (LEAVE A REPLY)
https://docs.splunk.com/Documentation/Splunk/7.3.1/Admin/Configurationfiledirectories Section titled, Configuration file directories, states "A detailed list of settings for each configuration file is provided in the .spec file names for that configuration file. You can find the latest version of the .spec and .example files in the $SPLUNK_HOME/etc system/README folder of your Splunk Enterprise installation..."

NEW QUESTION: 52
What type of data is counted against the Enterprise license at a fixed 150 bytes per event?
A. Internal Windows logs
B. Metricsdata
C. License data
D. Internal Splunk data
Answer: B (LEAVE A REPLY)

NEW QUESTION: 53
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. ignoreOlderThan = 45d
B. includeNewerThan = -35d
C. followTail = -45d
D. ignore = 45d
Answer: (SHOW ANSWER)

NEW QUESTION: 54
Which additional component is required for a search head cluster?
A. Monitoring Console
B. Deployer
C. Management Console
D. Cluster Master
Answer: B (LEAVE A REPLY)

NEW QUESTION: 55
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. A list of props. conf configurations as they are on-disk along with a file path from which the configuration is located
B. list of all the configurations on-disk that Splunk contains.
C. A verbose list of all configurations as they were when splunkd started.
D. A list of the current running props, conf configurations along with a file path from which the configuration was made
Answer: (SHOW ANSWER)

NEW QUESTION: 56
What action is required to enable forwarder management in Splunk Web?
A. Navigate to Settings > Server Settings > General Settings, and set an App server port.
B. Place an app in the SPLUNK_HOME/etc/deployment-apps directory of the deployment server.
C. Navigate to Settings > Forwarding and receiving, and click on Enable Forwarding.
D. Create a server class and map it to a client in SPLUNK_HOME/etc/system/local/serverclass.conf.
Answer: D (LEAVE A REPLY)

NEW QUESTION: 57
An index stores its data in buckets. Which default directories does Splunk use to store buckets? (Choose all that apply.)
A. frozendb
B. db
C. bucketdb
D. colddb
Answer: A,D (LEAVE A REPLY)

NEW QUESTION: 58
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)
Reference:
Configuretheuniversalforwarder

NEW QUESTION: 59
Which of the following applies only to Splunk index data integrity check?
A. Lookup table
B. Raw data in the index
C. Data model acceleration
D. Summary Index
Answer: B (LEAVE A REPLY)

NEW QUESTION: 60
Which of the following statements apply to directory inputs? {select all that apply)
A. Splunk recursively traverses through the directory structure.
B. When adding new log files to a monitored directory, the forwarder must be restarted to take them into account.
C. Compressed files are ignored by default
D. All discovered text files are consumed.
Answer: A,D (LEAVE A REPLY)

NEW QUESTION: 61
Which feature in Splunk allows Event Breaking, Timestamp extractions, and any advanced configurations found in props.conf to be validated all through the UI?
A. Apps
B. Search
C. Data preview
D. Forwarder inputs
Answer: C (LEAVE A REPLY)
http://www.splunk.com/view/SP-CAAAGPR

NEW QUESTION: 62
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)
Reference:
Configurationparametersandthedatapipeline

NEW QUESTION: 63
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.
Answer: A (LEAVE A REPLY)
https://docs.splunk.com/Documentation/Splunk/8.0.4/Data/Whitelistorblacklistspecificincomingdata
"It is not necessary to define both an allow list and a deny list in a configuration stanza. The settings are independent. If you do define both filters and a file matches them both, Splunk Enterprise does not index that file, as the blacklist filter overrides the whitelist filter." Source:
https://docs.splunk.com/Documentation/Splunk/8.1.0/Data/Whitelistorblacklistspecificincomingdata

NEW QUESTION: 64
Which of the following is accurate regarding the input phase?
A. Fine-tunes metadata.
B. Performs character encoding.
C. Breaks data into events with timestamps.
D. Applies event-level transformations.
Answer: A (LEAVE A REPLY)

NEW QUESTION: 65
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. linecount
B. splunk_server
C. index
D. host
Answer: B (LEAVE A REPLY)

NEW QUESTION: 66
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: (SHOW ANSWER)
https://docs.splunk.com/Documentation/Splunk/8.0.1/Forwarding/Aboutforwardingandreceivingdata
https://docs.splunk.com/Documentation/Forwarder/8.1.1/Forwarder/Configureforwardingwithoutputs.conf#:~:text=compressed%3Dtrue%20This%20tells%20the,the%20forwarder%20sends%20raw%20data.

NEW QUESTION: 67
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/maillog and /var/log/messages
B. /var/log/maillog
C. none of the above
D. /var/log/messages
Answer: B (LEAVE A REPLY)

NEW QUESTION: 68
How can native authentication be disabled in Splunk?
A. Set nativeAuthentication=false in authentication.conf
B. Remove the $SPLUNK_HOME/etc/passwd file
C. Create an empty $SPLUNK_HOME/etc/passwd file
D. Set SPLUNK_AUTHENTICATION=false in splunk-launch.conf
Answer: (SHOW ANSWER)

NEW QUESTION: 69
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: 70
Which setting in indexes. conf allows data retention to be controlled by time?
A. maxDaysToKeep
B. moveToFrozenAfter
C. maxDataRetentionTime
D. frozenTimePeriodInSecs
Answer: D (LEAVE A REPLY)
Explanation
https://docs.splunk.com/Documentation/Splunk/latest/Indexer/Setaretirementandarchivingpolicy

NEW QUESTION: 71
In which Splunk configuration is the SEDCMD used?
A. props, conf
B. inputs.conf
C. transforms.conf
D. indexes.conf
Answer: A (LEAVE A REPLY)

NEW QUESTION: 72
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
Answer: A (LEAVE A REPLY)
Explanation/Reference: https://answers.splunk.com/answers/371099/how-to-configure-deployment-apps-to-push-to- client.html

NEW QUESTION: 73
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: (SHOW ANSWER)
because transforms.conf is the right configuration file to state the regex expression. https://docs.splunk.com/Documentation/Splunk/8.1.0/Admin/Transformsconf Reference: 433035

NEW QUESTION: 74
When running the command shown below, what is the default path in which deployment server. conf is created?
splunk set deploy-poll deployServer:port
A. SFLUNK_HOME/etc/deployment
B. SPLUNK_HOME/etc/system/local
C. SPLUNK_KOME/etc/apps/deployment
D. SPLUNK_HOME/etc/system/default
Answer: (SHOW ANSWER)

NEW QUESTION: 75
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, deployment server, license master, universal forwarder, heavy forwarder
B. Indexers, search head, universal forwarders, license master
C. Indexers, search head, deployment server, universal forwarders
D. Indexers, search head, deployment server, license master, universal forwarder
Answer: D (LEAVE A REPLY)

NEW QUESTION: 76
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)

NEW QUESTION: 77
The universal forwarder has which capabilities when sending data? (select all that apply)
A. Obfuscating/hiding data
B. Compressing data
C. Indexer acknowledgement
D. Sending alerts
Answer: (SHOW ANSWER)

NEW QUESTION: 78
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: (SHOW ANSWER)
Explanation/Reference: https://docs.splunk.com/Documentation/Splunk/7.3.1/Security/ Aboutusersandroles#How_users_inherit_capabilities

NEW QUESTION: 79
With authentication methods are natively supported within Splunk Enterprise? (Choose all that apply.)
A. LDAP
B. SAML
C. RADIUS
D. Duo Multifactor Authentication
Answer: (SHOW ANSWER)
Explanation/Reference: https://docs.splunk.com/Documentation/Splunk/7.3.1/Security/SetupuserauthenticationwithSplunk

NEW QUESTION: 80
Which of the following statements accurately describes using SSL to secure the feed from a forwarder?
A. SSL automatically compresses the feed by default.
B. It requires that the receiver be set to compression=true.
C. It does not encrypt the certificate password.
D. It requires that the forwarder be set to compressed=true.

Answer: C (LEAVE A REPLY)

NEW QUESTION: 81
Which of the following monitor inputs stanza headers would match all of the following files?
/var/log/www1/secure.log
/var/log/www/secure.l
/var/log/www/logs/secure.logs
/var/log/www2/secure.log
A. [monitor:///var/log/www1/secure.log]
B. [monitor:///var/log/.../secure.*
C. [monitor:///var/log/www1/secure.*]
D. [monitor:///var/log/www*/secure.*]
Answer: A (LEAVE A REPLY)

NEW QUESTION: 82
What is the default value of LINE_BREAKER?
A. \r\n
B. ([\r\n]+)
C. (\r\n+)
D. \r+\n+
Answer: B (LEAVE A REPLY)

NEW QUESTION: 83
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: 84
After how many warnings within a rolling 30-day period will a license violation occur with an enforced Enterprise license?
A. 4
B. 5
C. 3
D. 1
Answer: B (LEAVE A REPLY)

NEW QUESTION: 85
What options are available when creating custom roles? (select all that apply)
A. Restrict search terms
B. Whitelist search terms
C. Limit the number of concurrent search jobs
D. Allow or restrict indexes that can be searched.
Answer: D (LEAVE A REPLY)

NEW QUESTION: 86
Which of the following authentication types requires scripting in Splunk?
A. ADFS
B. LDAP
C. SAML
D. RADIUS
Answer: D (LEAVE A REPLY)
Explanation/Reference: https://answers.splunk.com/answers/131127/scripted-authentication.html

NEW QUESTION: 87
What is the command to reset the fishbucket for one source?
A. splunk cmd btprobe -d SPLUNK_HOME/var/lib/splunk/fishbucket/splunk_private_db --file <source> --reset
B. rm -r ~/splunkforwarder/var/lib/splunk/fishbucket
C. splunk btool fishbucket reset <source>
D. splunk clean eventdata -index _thefishbucket
Answer: (SHOW ANSWER)

NEW QUESTION: 88
Which of the following statements apply to directory inputs? {select all that apply)
A. Splunk recursively traverses through the directory structure.
B. Compressed files are ignored by default
C. When adding new log files to a monitored directory, the forwarder must be restarted to take them into account.
D. All discovered text files are consumed.
Answer: (SHOW ANSWER)

NEW QUESTION: 89
Which Splunk component distributes apps and certain other configuration updates to search head cluster members?
A. Search head cluster master
B. Deployment server
C. Deployer
D. Cluster master
Answer: A (LEAVE A REPLY)

NEW QUESTION: 90
Which Splunk component does a search head primarily communicate with?
A. Indexer
B. Forwarder
C. Cluster master
D. Deployment server
Answer: (SHOW ANSWER)
Explanation/Reference: https://docs.splunk.com/Documentation/Splunk/7.3.1/InheritedDeployment/Deploymenttopology

NEW QUESTION: 91
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. Forward option
D. Upload option
Answer: D (LEAVE A REPLY)

NEW QUESTION: 92
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)
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: 93
The priority of layered Splunk configuration files depends on the file's:
A. Owner
B. Weight

C. Context

D. Creation time

Answer: C (LEAVE A REPLY)

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

NEW QUESTION: 94

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. none of the above

C. /var/log/maillog

D. /var/log/maillog and /var/log/messages

Answer: C (LEAVE A REPLY)

NEW QUESTION: 95

Which Splunk component requires a Forwarder license?

A. Heaviest forwarder

B. Heavy forwarder

C. Search head

D. Universal forwarder

Answer: B (LEAVE A REPLY)

NEW QUESTION: 96

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

A. maxDaysToKeep

B. moveToFrozenAfter

C. maxDataRetentionTime

D. frozenTimePeriodInSecs

Answer: D (LEAVE A REPLY)

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

NEW QUESTION: 97
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
Answer: (SHOW ANSWER)
https://docs.splunk.com/Documentation/Splunk/8.1.1/Data/Monitornetworkports Reference:
Bypassautomaticsourcetypeassignment

NEW QUESTION: 98
What hardware attribute would need to be changed to increase the number of simultaneous searches (ad-hoc and scheduled) on a single search head?
A. Network interface cards
B. CPUs
C. Disk
D. Memory
Answer: C (LEAVE A REPLY)

NEW QUESTION: 99
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: (SHOW ANSWER)
https://docs.splunk.com/Documentation/Splunk/latest/Security/Aboutusersandroles#Role_inheritance
https://docs.splunk.com/Documentation/Splunk/7.3.1/Security/Aboutusersandroles#How_users_inherit_capabilities

NEW QUESTION: 100
Which of the following indexes come pre-configured with Splunk Enterprise? (select all that apply)
A. _license
B. _Internal

C. _external
D. _thefishbucket
Answer: B,D (LEAVE A REPLY)
https://docs.splunk.com/Documentation/Splunk/8.0.5/Indexer/Howindexingworks

NEW QUESTION: 101
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)
Explanation/Reference: https://docs.splunk.com/Documentation/Splunk/7.3.1/Updating/Filterclients

NEW QUESTION: 102
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: (SHOW ANSWER)
Explanation/Reference: https://docs.splunk.com/Documentation/Splunk/7.3.1/Admin/User-seedconf

NEW QUESTION: 103
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)
Reference:
166653

NEW QUESTION: 104
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: 105
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: (SHOW ANSWER)
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: 106
What is required when adding a native user to Splunk? (select all that apply)
A. Password
B. Default app
C. Username
D. Full Name
Answer: A,C (LEAVE A REPLY)

NEW QUESTION: 107
Which of the following is an appropriate description of a deployment server in a non-cluster environment?
A. Allows management of local Splunk instances, requires Enterprise license, handles job of sending configurations packaged as apps. can automatically restart remote Splunk instances.
B. Allows management of remote Splunk instances, requires Enterprise license, handles job of sending configurations, can automatically restart remote Splunk instances.
C. Allows management of remote Splunk instances, requires no license, handles job of sending configurations, can automatically restart remote Splunk instances.
D. Allows management of remote Splunk instances, requires Enterprise license, handles job of sending configurations, can manually restart remote Splunk instances.
Answer: B (LEAVE A REPLY)
Reference:
https://docs.splunk.com/Documentation/Splunk/8.2.2/Updating/Deploymentserverarchitecture
"A deployment client is a Splunk instance remotely configured by a deployment server".

NEW QUESTION: 108
Which Splunk component requires a Forwarder license?
A. Heavy forwarder
B. Search head
C. Universal forwarder
D. Heaviest forwarder
Answer: C (LEAVE A REPLY)

NEW QUESTION: 109
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: (SHOW ANSWER)
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: 110
Which of the following enables compression for universal forwarders in outputs. conf ?
A)

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

B)

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

C)

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

D)

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

A. Option D
B. Option A
C. Option B
D. Option C
Answer: (SHOW ANSWER)

NEW QUESTION: 111
Within props. conf, which stanzas are valid for data modification? (select all that apply)
A. Sourcetype
B. Server
C. Source
D. Host
Answer: A,C,D (LEAVE A REPLY)

NEW QUESTION: 112
Which layers are involved in Splunk configuration file layering? (select all that apply)
A. App context
B. User context
C. Global context
D. Forwarder context
Answer: A,B,C (LEAVE A REPLY)
https://docs.splunk.com/Documentation/Splunk/latest/Admin/Wheretofindtheconfigurationfiles To determine the order of directories for evaluating configuration file precedence, Splunk software considers each file's context. Configuration files operate in either a global context or in the context of the current app and user: Global. Activities like indexing take place in a global context. They are independent of any app or user. For example, configuration files that determine monitoring or indexing behavior occur outside of the app and user context and are global in nature. App/user. Some activities, like searching, take place in an app or user context. The app and user context is vital to search-time processing, where certain knowledge objects or actions might be valid only for specific users in specific apps.

NEW QUESTION: 113
Which forwarder is recommended by Splunk to use in a production environment?
A. Heavy forwarder
B. Universal forwarder
C. Lightweight forwarder
D. SSL forwarder
Answer: (SHOW ANSWER)

NEW QUESTION: 114
Which parent directory contains the configuration files in Splunk?
A. SSPLUNK_HCME/var

B. SSPLUNK_HOME/conf
C. SSPLUNK_HOME/default
D. SSFLUNK_KOME/etc
Answer: D (LEAVE A REPLY)

NEW QUESTION: 115
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-xxxAcct = s/AcctID=\d{3}(\d{4})/AcctID=xxx/g
B. SEDCMD-1acct = s/VendorID=\d{3}(\d{4})/VendorID=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
Answer: (SHOW ANSWER)

NEW QUESTION: 116
Which optional configuration setting in inputs .conf allows you to selectively forward the data to specific indexer(s)?
A. _INDEXER_LIST
B. _INDEXER_GROUP
C. _INDEXER ROUTING
D. _TCP_ROUTING
Answer: D (LEAVE A REPLY)

NEW QUESTION: 117
Which of the following is a valid distributed search group?
A. [distributedSearch:Paris] default = false servers = server1:8089; server2:8089
B. [searchGroup:Paris] default = false servers = server1:8089, server2:8089
C. [distributedSearch:Paris] default = false servers = server1, server2
D. [searchGroup:Paris] default = false servers = server1:9997, server2:9997
Answer: A (LEAVE A REPLY)

NEW QUESTION: 118
When Splunk is integrated with LDAP, which attribute can be changed in the Splunk UI for an LDAP user?
A. Default app
B. LDAP group
C. Username
D. Password
Answer: B (LEAVE A REPLY)

NEW QUESTION: 119
Which feature of Splunk's role configuration can be used to aggregate multiple roles intended for groups of users?

A. Role federation
B. Role inheritance
C. Linked roles
D. Grantable roles
Answer: B (LEAVE A REPLY)

NEW QUESTION: 120
When configuring HTTP Event Collector (HEC) input, how would one ensure the events have been indexed?
A. Enable indexer acknowledgment.
B. Enable forwarder acknowledgment.
C. splunk check-integrity -index <index name>
D. index=_internal component=ACK | stats count by host
Answer: A (LEAVE A REPLY)
Reference https://docs.splunk.com/Documentation/Splunk/8.0.5/Data/AboutHECIDXAck