Splunk.SPLK-1003.v2025-02-04.q185

Exam Code:	SPLK-1003
Exam Name:	Splunk Enterprise Certified Admin
Certification Provider:	Splunk
Free Question Number:	185
Version:	v2025-02-04
# of views:	22896
# of Questions views:	11824
https://www.dumpsfiles.com/files/Splunk/SPLK-1003/Splunk.SPLK-1003.v2025-02-04.q185	

NEW QUESTION: 1
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 precendence, Splunk software considers each file's context. Configuration files operate in either a global context or in the context of the current app and user"

NEW QUESTION: 2
Which of the following describes a Splunk deployment server?
A. A Splunk Forwarder that deploys data to multiple indexers.
B. A Splunk app installed on a Splunk Enterprise server.
C. A Splunk Enterprise server that distributes apps.
D. A server that automates the deployment of Splunk Enterprise to remote servers.
Answer: C (LEAVE A REPLY)
A Splunk deployment server is a system that distributes apps, configurations, and other assets to groups of Splunk Enterprise instances. You can use it to distribute updates to most types of Splunk Enterprise components: forwarders, non-clustered indexers, and search heads2.
A Splunk deployment server is available on every full Splunk Enterprise instance. To use it, you must activate it by placing at least one app into %SPLUNK_HOME%\etc\deployment-apps on the host you want to act as deployment server3.
A Splunk deployment server maintains the list of server classes and uses those server classes to determine what content to distribute to each client. A server class is a group of deployment clients that share one or more defined characteristics1.
A Splunk deployment client is a Splunk instance remotely configured by a deployment server. Deployment clients can be universal forwarders, heavy forwarders, indexers, or search heads. Each deployment client belongs to one or more server classes1.

A Splunk deployment app is a set of content (including configuration files) maintained on the deployment server and deployed as a unit to clients of a server class. A deployment app can be an existing Splunk Enterprise app or one developed solely to group some content for deployment purposes1.
Therefore, option C is correct, and the other options are incorrect.

NEW QUESTION: 3
Search heads in a company's European offices need to be able to search data in their New York offices. They also need to restrict access to certain indexers. What should be configured to allow this type of action?
A. Indexer clustering
B. LDAP control
C. Distributed search
D. Search head clustering
Answer: (SHOW ANSWER)
The correct answer is C. Distributed search is the feature that allows search heads in a company's European offices to search data in their New York offices. Distributed search also enables restricting access to certain indexers by using the splunk_server field or the server.conf file1.
Distributed search is a way to scale your Splunk deployment by separating the search management and presentation layer from the indexing and search retrieval layer. With distributed search, a Splunk instance called a search head sends search requests to a group of indexers, or search peers, which perform the actual searches on their indexes. The search head then merges the results back to the user2.
Distributed search has several use cases, such as horizontal scaling, access control, and managing geo-dispersed data. For example, users in different offices can search data across the enterprise or only in their local area, depending on their needs and permissions2.
The other options are incorrect because:
A) Indexer clustering is a feature that replicates data across a group of indexers to ensure data availability and recovery. Indexer clustering does not directly affect distributed search, although search heads can be configured to search across an indexer cluster3.
B) LDAP control is a feature that allows Splunk to integrate with an external LDAP directory service for user authentication and role mapping. LDAP control does not affect distributed search, although it can be used to manage user access to data and searches.
D) Search head clustering is a feature that distributes the search workload across a group of search heads that share resources, configurations, and jobs. Search head clustering does not affect distributed search, although the search heads in a cluster can search across the same set of indexers.

NEW QUESTION: 4
Which Splunk component distributes apps and certain other configuration updates to search head cluster members?
A. Search head cluster master
B. Cluster master
C. Deployment server
D. Deployer
Answer: D (LEAVE A REPLY)

NEW QUESTION: 5
Which valid bucket types are searchable? (select all that apply)
A. Cold buckets
B. Frozen buckets
C. Warm buckets
D. Hot buckets

Answer: C (LEAVE A REPLY)

NEW QUESTION: 6
The universal forwarder has which capabilities when sending data? (select all that apply)
A. Obfuscating/hiding data
B. Compressing data
C. Sending alerts
D. Indexer acknowledgement
Answer: (SHOW ANSWER)

NEW QUESTION: 7
Which of the following are available input methods when adding a file input in Splunk Web? (Choose all that apply.)
A. Index once.
B. Monitor interval.
C. On-demand monitor.
D. Continuously monitor.
Answer: (SHOW ANSWER)
Explanation
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: 8
Windows can prevent a Splunk forwarder from reading open files. If files need to be read while they are being written to, what type of input stanza needs to be created?
A. Tail Reader
B. Upload
C. MonitorNoHandle
D. Monitor
Answer: C (LEAVE A REPLY)
The correct answer is C. MonitorNoHandle.
MonitorNoHandle is a type of input stanza that allows a Splunk forwarder to read files on Windows systems as Windows writes to them. It does this by using a kernel-mode filter driver to capture raw data as it gets written to the file1. This input stanza is useful for files that get locked open for writing, such as the Windows DNS server log file2.
The other options are incorrect because:
A) Tail Reader is not a valid input stanza in Splunk. It is a component of the Tailing Processor, which is responsible for monitoring files and directories for new data3.
B) Upload is a type of input stanza that allows Splunk to index a single file from a local or network file system. It is not suitable for files that are constantly being updated, as it only indexes the file once and does not monitor it for changes4.
D) Monitor is a type of input stanza that allows Splunk to monitor files and directories for new data. However, it may not work for files that Windows prevents Splunk from reading while they are open. In such cases, MonitorNoHandle is a better option2.

A Splunk forwarder is a lightweight agent that can forward data to a Splunk deployment. There are two types of forwarders: universal and heavy. A universal forwarder can only forward data, while a heavy forwarder can also perform parsing, filtering, routing, and aggregation on the data before forwarding it5.
An input stanza is a section in the inputs.conf configuration file that defines the settings for a specific type of input, such as files, directories, network ports, scripts, or Windows event logs. An input stanza starts with a square bracket, followed by the input type and the input path or name. For example, [monitor:///var/log] is an input stanza for monitoring the /var/log directory.
Reference:
1: Monitor files and directories - Splunk Documentation
2: How to configure props.conf for proper line breaking ... - Splunk Community
3: How Splunk Enterprise monitors files and directories - Splunk Documentation
4: Upload a file - Splunk Documentation
5: Use forwarders to get data into Splunk Enterprise - Splunk Documentation
[6]: inputs.conf - Splunk Documentation

NEW QUESTION: 9
The CLI command splunk add forward-server indexer:<receiving-port> will create stanza(s) in which configuration file?
A. inputs.conf
B. indexes.conf
C. outputs.conf
D. servers.conf
Answer: C (LEAVE A REPLY)
The CLI command "Splunk add forward-server indexer:<receiving-port>" is used to define the indexer and the listening port on forwards. The command creates this kind of entry "[tcpout-server://<ip address>:<port>]" in the outputs.conf file.
https://docs.splunk.com/Documentation/Forwarder/8.2.2/Forwarder/Configureforwardingwithoutputs.conf

NEW QUESTION: 10
Which option accurately describes the purpose of the HTTP Event Collector (HEC)?
A. A token-based HTTP input that is insecure and non-scalable and that does not require the use of forwarders.
B. A token-based HTTP input that is secure and scalable and that requires 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 secure and scalable and that does not require the use of forwarders.
Answer: B (LEAVE A REPLY)

NEW QUESTION: 11
When running the command shown below, what is the default path in which deployment server. conf is created?
splunk set deploy-poll deployServer:port
A. SFLUNK_HOME/etc/deployment
B. SPLUNK_HOME/etc/system/local
C. SPLUNK_HOME/etc/system/default
D. SPLUNK_KOME/etc/apps/deployment
Answer: C (LEAVE A REPLY)
Explanation
https://docs.splunk.com/Documentation/Splunk/8.1.1/Updating/Definedeploymentclasses#Ways_to_define_serv

"When you use forwarder management to create a new server class, it saves the server class definition in a copy of serverclass.conf under $SPLUNK_HOME/etc/system/local. If, instead of using forwarder management, you decide to directly edit serverclass.conf, it is recommended that you create the serverclass.conf file in that same directory, $SPLUNK_HOME/etc/system/local."

NEW QUESTION: 12
Where should apps be located on the deployment server that the clients pull from?
A. $SPLUNK_HCME/etc/master-apps
B. $SPLUNK_HCME/etc/sear:ch
C. $SPLUNK HCME/etc/deployment-apps
D. $SFLUNK_KOME/etc/apps
Answer: (SHOW ANSWER)

NEW QUESTION: 13
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 Local Windows network monitoring.
C. Use an index with an Index Data Type of Metrics.
D. Use Windows Remote Inputs with WMI.
Answer: (SHOW ANSWER)

NEW QUESTION: 14
An add-on has configured field aliases for source IP address and destination IP address fields. A specific user prefers not to have those fields present in their user context. Based on the default props.conf below, which SPLUNK_HOME/etc/users/buttercup/myTA/local/props.conf stanza can be added to the user's local context to disable the field aliases?

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

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

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

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

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

dumpsfiles.com

A. Option A
B. Option B
C. Option C
D. Option D
Answer: (SHOW ANSWER)
https://docs.splunk.com/Documentation/Splunk/latest/Admin/Howtoeditaconfigurationfile#Clear%20a%20setting

NEW QUESTION: 15
Within props. conf, which stanzas are valid for data modification? (select all that apply)
A. Host
B. Server
C. Source
D. Sourcetype
Answer: A,C,D (LEAVE A REPLY)
Explanation
https://docs.splunk.com/Documentation/Splunk/8.0.4/Admin/Propsconf#props.conf.spec
https://docs.splunk.com/Documentation/Splunk/8.1.1/Admin/Propsconf
"* Reuse of the same field-extracting regular expression across multiple sources, source types, or hosts."
https://docs.splunk.com/Documentation/Splunk/8.0.4/Admin/Propsconf#props.conf.spec

NEW QUESTION: 16
Which of the following statements describe deployment management? (select all that apply)
A. Requires an Enterprise license
B. Is responsible for sending apps to forwarders.

C. Once used, is the only way to manage forwarders
D. Can automatically restart the host OS running the forwarder.
Answer: A,B (LEAVE A REPLY)
https://docs.splunk.com/Documentation/Splunk/8.2.2/Admin/Distdeploylicenses#:~:text=License%20requirements,do%20not%20index%20external%20data.
"All Splunk Enterprise instances functioning as management components needs access to an Enterprise license. Management components include the deployment server, the indexer cluster manager node, the search head cluster deployer, and the monitoring console."
https://docs.splunk.com/Documentation/Splunk/8.2.2/Updating/Aboutdeploymentserver
"The deployment server is the tool for distributing configurations, apps, and content updates to groups of Splunk Enterprise instances."

Valid SPLK-1003 Dumps shared by TrainingDump.com for Helping Passing SPLK-1003 Exam! TrainingDump.com now offer the **newest SPLK-1003 exam dumps**, the TrainingDump.com SPLK-1003 exam **questions have been updated** and **answers have been corrected** get the **newest** TrainingDump.com SPLK-1003 dumps with Test Engine here:
https://www.trainingdump.com/Splunk/SPLK-1003-practice-exam-dumps.html (**232** Q&As Dumps, **40%OFF** **Special Discount:** **Exam-Tests**)

NEW QUESTION: 17
In which phase of the index time process does the license metering occur?
A. Parsing phase
B. input phase
C. Indexing phase
D. Licensing phase
Answer: C (LEAVE A REPLY)

NEW QUESTION: 18
In this source definition the MAX_TIMESTAMP_LOOKHEAD is missing. Which value would fit best?

```
[sshd_syslog]
TIME_PREFIX = ^
TIME_FORMAT = %Y-%m-%d %H:%M:%S.%3N %z
LINE_BREAKER = ([\r\n]+)\d{4}-\d{2}-\d{2} \d{2}:\d{2}:\d{2}
SHOULD_LINEMERGE = false
TRUNCATE = 0
```

Event example:

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

A. MAX_TIMESTAMF_LOOKHEAD = 20
B. MAX TIMESTAMP LOOKAHEAD - 30
C. MAX_TIMESTAMP_LOOKAHEAD - 10
D. MAX_TIMESTAMP_L0CKAHEAD = 5
Answer: B (LEAVE A REPLY)

NEW QUESTION: 19
On the deployment server, administrators can map clients to server classes using client filters. Which of the following statements is accurate?
A. The blacklist takes precedence over the whitelist.

B. The whitelist takes precedence over the blacklist.
C. Wildcards are not supported in any client filters.
D. Machine type filters are applied before the whitelist and blacklist.
Answer: A (LEAVE A REPLY)
Reference:
same/td-p/390910

NEW QUESTION: 20
Which parent directory contains the configuration files in Splunk?
A. SSPLUNK_HCME/var
B. SSPLUNK_HOME/default
C. SSFLUNK_KOME/etc
D. SSPLUNK_HOME/conf
Answer: C (LEAVE A REPLY)

NEW QUESTION: 21
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: B (LEAVE A REPLY)
Explanation/Reference: https://docs.splunk.com/Documentation/Forwarder/7.3.1/Forwarder/Configuretheuniversalforwarder

NEW QUESTION: 22
Which default Splunk role could be assigned to provide users with the following capabilities?
Create saved searches
Edit shared objects and alerts
Not allowed to create custom roles
A. power
B. splunk-system-role
C. user
D. admin
Answer: A (LEAVE A REPLY)

NEW QUESTION: 23
What is the valid option for a [monitor] stanza in inputs.conf?
A. enabled
B. datasource
C. server_name
D. ignoreOlderThan

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

NEW QUESTION: 24
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: 25
User role inheritance allows what to be inherited from the parent role? (Select all that apply.)
A. Parents
B. Capabilities
C. Index access
D. Search history
Answer: B (LEAVE A REPLY)
Explanation/Reference: https://docs.splunk.com/Documentation/Splunk/7.3.1/Security/ Aboutusersandroles#How_users_inherit_capabilities

NEW QUESTION: 26
Which of the following authentication types requires scripting in Splunk?
A. ADFS
B. LDAP
C. SAML
D. RADIUS
Answer: D (LEAVE A REPLY)
https://answers.splunk.com/answers/131127/scripted-authentication.html
Scripted Authentication: An option for Splunk Enterprise authentication. You can use an authentication system that you have in place (such as PAM or RADIUS) by configuring authentication.conf to use a script instead of using LDAP or Splunk Enterprise default authentication.

NEW QUESTION: 27
Which pathway represents where a network input in Splunk might be found?
A. $SPLUNK HOME/ etc/ apps/ ne two r k/ inputs.conf
B. $SPLUNK HOME/ etc/ apps/ $appName/ local / inputs.conf
C. $SPLUNK HOME/ system/ local /udp.conf

D. $SPLUNK HOME/ var/lib/ splunk/$inputName/homePath/

Answer: (SHOW ANSWER)

The correct answer is B. The network input in Splunk might be found in the $SPLUNK_HOME/etc/apps/$appName/local/inputs.conf file.

A network input is a type of input that monitors data from TCP or UDP ports. To configure a network input, you need to specify the port number, the connection host, the source, and the sourcetype in the inputs.conf file. You can also set other optional settings, such as index, queue, and host_regex1.

The inputs.conf file is a configuration file that contains the settings for different types of inputs, such as files, directories, scripts, network ports, and Windows event logs. The inputs.conf file can be located in various directories, depending on the scope and priority of the settings. The most common locations are:

$SPLUNK_HOME/etc/system/default: This directory contains the default settings for all inputs. You should not modify or copy the files in this directory2.

$SPLUNK_HOME/etc/system/local: This directory contains the custom settings for all inputs that apply to the entire Splunk instance. The settings in this directory override the default settings2.

$SPLUNK_HOME/etc/apps/$appName/default: This directory contains the default settings for all inputs that are specific to an app. You should not modify or copy the files in this directory2.

$SPLUNK_HOME/etc/apps/$appName/local: This directory contains the custom settings for all inputs that are specific to an app. The settings in this directory override the default and system settings2.

Therefore, the best practice is to create or edit the inputs.conf file in the $SPLUNK_HOME/etc/apps/$appName/local directory, where $appName is the name of the app that you want to configure the network input for. This way, you can avoid modifying the default files and ensure that your settings are applied to the specific app.

The other options are incorrect because:

A) There is no network directory under the apps directory. The network input settings should be in the inputs.conf file, not in a separate directory.

C) There is no udp.conf file in Splunk. The network input settings should be in the inputs.conf file, not in a separate file. The system directory is not the recommended location for custom settings, as it affects the entire Splunk instance.

D) The var/lib/splunk directory is where Splunk stores the indexed data, not the input settings. The homePath setting is used to specify the location of the index data, not the input data. The inputName is not a valid variable for inputs.conf.

NEW QUESTION: 28

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

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

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

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

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

Answer: C (LEAVE A REPLY)

NEW QUESTION: 29

The Splunk administrator wants to ensure data is distributed evenly amongst the indexers. To do this, he runs the following search over the last 24 hours:

index=*

What field can the administrator check to see the data distribution?

A. host

B. index

C. linecount

D. splunk_server

Answer: D (LEAVE A REPLY)

NEW QUESTION: 30

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

A. Metricsdata
B. License data
C. Internal Windows logs
D. Internal Splunk data
Answer: A (LEAVE A REPLY)

NEW QUESTION: 31
When deploying apps on Universal Forwarders using the deployment server, what is the correct component and location of the app before it is deployed?
A. On Universal Forwarder, $SPLUNK_HOME/etc/apps
B. On Deployment Server, $SPLUNK_HOME/etc/apps
C. On Deployment Server, $SPLUNK_HOME/etc/deployment-apps
D. On Universal Forwarder, $SPLUNK_HOME/etc/deployment-apps
Answer: (SHOW ANSWER)
The correct answer is C. On Deployment Server, $SPLUNK_HOME/etc/deployment-apps.
A deployment server is a Splunk Enterprise instance that acts as a centralized configuration manager for any number of other instances, called "deployment clients". A deployment client can be a universal forwarder, a non-clustered indexer, or a search head1.
A deployment app is a directory that contains any content that you want to download to a set of deployment clients. The content can include a Splunk Enterprise app, a set of Splunk Enterprise configurations, or other content, such as scripts, images, and supporting files2.
You create a deployment app by creating a directory for it on the deployment server. The default location is $SPLUNK_HOME/etc/deployment-apps, but this is configurable through the repositoryLocation attribute in serverclass.conf. Underneath this location, each app must have its own subdirectory. The name of the subdirectory serves as the app name in the forwarder management interface2.
The other options are incorrect because:
A) On Universal Forwarder, $SPLUNK_HOME/etc/apps. This is the location where the deployment app resides after it is downloaded from the deployment server to the universal forwarder. It is not the location of the app before it is deployed2.
B) On Deployment Server, $SPLUNK_HOME/etc/apps. This is the location where the apps that are specific to the deployment server itself reside. It is not the location where the deployment apps for the clients are stored2.
D) On Universal Forwarder, $SPLUNK_HOME/etc/deployment-apps. This is not a valid location for any app on a universal forwarder. The universal forwarder does not act as a deployment server and does not store deployment apps3.

Valid SPLK-1003 Dumps shared by TrainingDump.com for Helping Passing SPLK-1003 Exam! TrainingDump.com now offer the **newest SPLK-1003 exam dumps**, the TrainingDump.com SPLK-1003 exam **questions have been updated** and **answers have been corrected** get the **newest** TrainingDump.com SPLK-1003 dumps with Test Engine here:
https://www.trainingdump.com/Splunk/SPLK-1003-practice-exam-dumps.html (**232** Q&As Dumps, **40%OFF** **Special Discount:** **Exam-Tests**)

NEW QUESTION: 32
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

Answer: D (LEAVE A REPLY)
Explanation/Reference: https://docs.splunk.com/Documentation/Splunk/7.3.1/Forwarding/Typesofforwarders

NEW QUESTION: 33
User role inheritance allows what to be inherited from the parent role? (select all that apply)
A. Parents
B. Capabilities
C. Index access
D. Search history
Answer: B,C (LEAVE A REPLY)
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: 34
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/default
C. SPLUNK_HOME/etc/system/local
D. SPLUNK_KOME/etc/apps/deployment
Answer: B (LEAVE A REPLY)

NEW QUESTION: 35
To set up a network input in Splunk, what needs to be specified?
A. File path.
B. Username and password.
C. Network protocol and port number.
D. Network protocol and MAC address.
Answer: A (LEAVE A REPLY)
Explanation/Reference: http://dev.splunk.com/view/dev-guide/SP-CAAAE3A

NEW QUESTION: 36
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.
Answer: C (LEAVE A REPLY)
Explanation
URLhttps://docs.splunk.com/Documentation/Splunk/8.2.2/DistSearch/Configuredistributedsearch
"To activate distributed search, you add search peers, or indexers, to a Splunk Enterprise instance that you desingate as a search head. You do this by specifying each search peer manually."

NEW QUESTION: 37
Which Splunk component does a search head primarily communicate with?
A. Forwarder
B. Deployment server
C. Cluster master
D. Indexer
Answer: (SHOW ANSWER)

NEW QUESTION: 38
A new forwarder has been installed with a manually createddeploymentclient.conf.
What is the next step to enable the communication between the forwarder and the deployment server?
A. Restart Splunk on the deployment server.
B. Enable the deployment client in Splunk Web under Forwarder Management.
C. Restart Splunk on the deployment client.
D. Wait for up to the time set in thephoneHomeIntervalInSecssetting.
Answer: C (LEAVE A REPLY)
Explanation
The next step to enable the communication between the forwarder and the deployment server after installing a new forwarder with a manually created deploymentclient.conf is to restart Splunk on the deployment client.
The deploymentclient.conf file contains the settings for the deployment client, which is a Splunk instance that receives updates from the deployment server. The file must include the targetUri attribute, which specifies the hostname and management port of the deployment server. To apply the changes in the deploymentclient.conf file, Splunk must be restarted on the deployment client. Therefore, option C is the correct answer.
References: Splunk Enterprise Certified Admin | Splunk, [Configure deployment clients - Splunk Documentation]

NEW QUESTION: 39
What conf file needs to be edited to set up distributed search groups?
A. distsearch.conf
B. distibutedsearch.conf
C. props.conf
D. search.conf
Answer: (SHOW ANSWER)

NEW QUESTION: 40
What is the default character encoding used by Splunk during the input phase?
A. EBCDIC
B. UTF-16
C. UTF-8
D. ISO 8859
Answer: C (LEAVE A REPLY)

NEW QUESTION: 41
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: 42
When deploying apps, which attribute in the forwarder management interface determines the apps that clients install?
A. Client Class
B. App Class
C. Server Class
D. Forwarder Class
Answer: C (LEAVE A REPLY)

NEW QUESTION: 43
After an Enterprise Trial license expires, it will automatically convert to a Free license. How many days is an Enterprise Trial license valid before this conversion occurs?
A. 90 days
B. 60 days
C. 7 days
D. 14 days
Answer: (SHOW ANSWER)
Reference:
https://docs.splunk.com/Documentation/Splunk/8.2.3/Admin/TypesofSplunklicenses

NEW QUESTION: 44
Which of the following enables compression for universal forwarders in outputs. conf ?
A)

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

B)

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

C)

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

D)

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

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

NEW QUESTION: 45
Which of the following authentication types requires scripting in Splunk?
A. RADIUS
B. SAML
C. LDAP
D. ADFS
Answer: A (LEAVE A REPLY)

NEW QUESTION: 46
Load balancing on a Universal Forwarder is not scaling correctly. The forwarder's outputs. and the tcpout stanza are setup correctly. What else could be the cause of this scaling issue? (select all that apply)
A. The receiving port is not properly setup to listen on the right port.
B. The inputs . conf'S _SYSZOG_ROVTING is not setup to use the right group names.
C. The DNS record used is not setup with a valid list of IP addresses.
D. The indexAndForward value is not set properly.
Answer: A,C (LEAVE A REPLY)
The possible causes of the load balancing issue on the Universal Forwarder are A and C. The receiving port and the DNS record are both factors that affect the ability of the Universal Forwarder to distribute data across multiple receivers. If the receiving port is not properly set up to listen on the right port, or if the DNS record used is not set up with a valid list of IP addresses, the Universal Forwarder might fail to connect to some or all of the receivers, resulting in poor load balancing.

Valid SPLK-1003 Dumps shared by TrainingDump.com for Helping Passing SPLK-1003 Exam! TrainingDump.com now offer the **newest SPLK-1003 exam dumps**, the TrainingDump.com SPLK-1003 exam **questions have been updated** and **answers have been corrected** get the **newest** TrainingDump.com SPLK-1003 dumps with Test Engine here:
https://www.trainingdump.com/Splunk/SPLK-1003-practice-exam-dumps.html (**232** Q&As Dumps, **40%OFF** **Special Discount:** **Exam-Tests**)

NEW QUESTION: 47
Which of the following apply to how distributed search works? (Select all that apply.)
A. The search head dispatches searches to the peers.
B. The search peers pull the data from the forwarders.
C. Peers run searches in parallel and return their portion of results.
D. The search head consolidates the individual results and prepares reports.

Answer: A (LEAVE A REPLY)
Explanation/Reference: https://docs.splunk.com/Documentation/Splunk/7.3.1/DistSearch/Whatisdistributedsearch

NEW QUESTION: 48
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 B
C. Option C
D. Option A
Answer: A (LEAVE A REPLY)

NEW QUESTION: 49
Which data pipeline phase is the last opportunity for defining event boundaries?
A. Input phase
B. Indexing phase
C. Parsing phase
D. Search phase
Answer: C (LEAVE A REPLY)
Reference https://docs.splunk.com/Documentation/Splunk/8.2.3/Admin/Configurationparametersandthedatapipeline

NEW QUESTION: 50
Which setting allows the configuration of Splunk to allow events to span over more than one line?
A. SHOULD_LINEMERGE = true
B. BREAK_ONLY_BEFORE_DATE = true
C. BREAK_ONLY_BEFORE = <REGEX pattern>
D. SHOULD_LINEMERGE = false
Answer: A (LEAVE A REPLY)

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

NEW QUESTION: 51
When using a directory monitor input, specific source types can be selectively overridden using which configuration file?
A. sourcetypes . conf
B. trans forms . conf
C. outputs . conf
D. props . conf
Answer: D (LEAVE A REPLY)
When using a directory monitor input, specific source types can be selectively overridden using the props.conf file. According to the Splunk documentation1, "You can specify a source type for data based on its input and source. Specify source type for an input. You can assign the source type for data coming from a specific input, such as /var/log/. If you use Splunk Cloud Platform, use Splunk Web to define source types. If you use Splunk Enterprise, define source types in Splunk Web or by editing the inputs.conf configuration file." However, this method is not very granular and assigns the same source type to all data from an input. To override the source type on a per-event basis, you need to use the props.conf file and the transforms.conf file2. The props.conf file contains settings that determine how the Splunk platform processes incoming data, such as how to segment events, extract fields, and assign source types2. The transforms.conf file contains settings that modify or filter event data during indexing or search time2. You can use these files to create rules that match specific patterns in the event data and assign different source types accordingly2. For example, you can create a rule that assigns a source type of apache_error to any event that contains the word "error" in the first line2.

NEW QUESTION: 52
How do you remove missing forwarders from the Monitoring Console?
A. By reloading the deployment server.
B. By restarting Splunk.
C. By rescanning active forwarders.
D. By rebuilding the forwarder asset table.
Answer: C (LEAVE A REPLY)

NEW QUESTION: 53
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: 54
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
Answer: C (LEAVE A REPLY)
Explanation
"When ingesting event data, the measured data volume is based on the new raw data that is placed into the indexing pipeline. Because the data is measured at the indexing pipeline, data that is filetered and dropped prior to indexing does not count against the license volume qota."
https://docs.splunk.com/Documentation/Splunk/8.0.6/Admin/HowSplunklicensingworks

NEW QUESTION: 55
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: (SHOW ANSWER)
Explanation
"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: 56
When Splunk is integrated with LDAP, which attribute can be changed in the Splunk UI for an LDAP user?
A. Default app
B. LDAP group
C. Password
D. Username
Answer: A (LEAVE A REPLY)
When Splunk is integrated with LDAP, most of the user attributes are managed by the LDAP server and cannot be changed in the Splunk UI. However, one exception is the default app attribute, which specifies which app a user sees when they log in to Splunk. This attribute can be changed in the Splunk UI by editing the user settings. Therefore, option A is the correct answer.
Reference: Splunk Enterprise Certified Admin | Splunk, [Configure Splunk to use LDAP and map groups - Splunk Documentation]

NEW QUESTION: 57
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: (SHOW ANSWER)
Explanation
"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: 58
Local user accounts created in Splunk store passwords in which file?
A. $ SFLUNK_HOME/etc/passwd
B. $ SFLUNK_HOME/etc/authentication
C. $ S?LUNK_HOME/etc/users/passwd.conf
D. $ SPLUNK HOME/etc/users/authentication.conf
Answer: A (LEAVE A REPLY)
Explanation
Per the provided reference URLhttps://docs.splunk.com/Documentation/Splunk/7.3.1/Admin/User-seedconf
"To set the default username and password, place user-seed.conf in $SPLUNK_HOME/etc/system/local. You must restart Splunk to enable configurations. If the $SPLUNK_HOME/etc/passwd file is present, the settings in this file (user-seed.conf) are not used."

NEW QUESTION: 59
Which Splunk component would one use to perform line breaking prior to indexing?
A. Heavy Forwarder
B. Universal Forwarder
C. Search head
D. This can only be done at the indexing layer.
Answer: A (LEAVE A REPLY)
Explanation
According to the Splunk documentation1, a heavy forwarder is a Splunk Enterprise instance that can parse and filter data before forwarding it to an indexer. A heavy forwarder can perform line breaking, which is the process of splitting incoming data into individual events based on a set of rules2. A heavy forwarder can also apply other transformations to the data, such as field extractions, event type matching, or masking sensitive data3.

NEW QUESTION: 60
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: D (LEAVE A REPLY)
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: 61
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.
Answer: B (LEAVE A REPLY)
https://docs.splunk.com/Documentation/Splunk/8.0.6/Security/ManageSplunkuserroleswithLDAP

Valid SPLK-1003 Dumps shared by TrainingDump.com for Helping Passing SPLK-1003 Exam! TrainingDump.com now offer the **newest SPLK-1003 exam dumps**, the TrainingDump.com SPLK-1003 exam **questions have been updated** and **answers have been corrected** get the **newest** TrainingDump.com SPLK-1003 dumps with Test Engine here:
https://www.trainingdump.com/Splunk/SPLK-1003-practice-exam-dumps.html (**232** Q&As Dumps, **40%OFF** **Special Discount:** **Exam-Tests**)

NEW QUESTION: 62
Which of the following is accurate regarding the input phase?
A. Breaks data into events with timestamps.
B. Applies event-level transformations.
C. Fine-tunes metadata.
D. Performs character encoding.
Answer: D (LEAVE A REPLY)
https://docs.splunk.com/Documentation/Splunk/latest/Deploy/Datapipeline "The data pipeline segments in depth. INPUT - In the input segment, Splunk software consumes data. It acquires the raw data stream from its source, breaks it into 64K blocks, and annotates each block with some metadata keys. The keys can also include values that are used internally, such as the character encoding of the data stream, and values that control later processing of the data, such as the index into which the events should be stored. PARSING Annotating individual events with metadata copied from the source-wide keys. Transforming event data and metadata according to regex transform rules."

NEW QUESTION: 63
What is the correct curl to send multiple events through HTTP Event Collector?

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

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

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

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

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

NEW QUESTION: 64
Which configuration files are used to transform raw data ingested by Splunk? (Choose all that apply.)
A. props.conf
B. transforms.conf

C. inputs.conf
D. rawdata.conf
Answer: A (LEAVE A REPLY)

NEW QUESTION: 65
Which of the following are supported configuration methods to add inputs on a forwarder? (select all that apply)
A. Forwarder Management
B. Edit forwarder.conf
C. Edit inputs . conf
D. CLI
Answer: (SHOW ANSWER)

NEW QUESTION: 66
What happens when the same username exists in Splunk as well as through LDAP?
A. LDAP user is automatically deleted from authentication.conf
B. Splunk settings take precedence.
C. LDAP settings take precedence.
D. Splunk user is automatically deleted from authentication.conf.
Answer: (SHOW ANSWER)
Reference:
Splunk platform attempts native authentication first. If authentication fails outside of a local account that doesn't exist, there is no attempt to use LDAP to log in. This is adapted from precedence of Splunk authentication schema.

NEW QUESTION: 67
The following stanza is active in indexes.conf:
[cat_facts]
maxHotSpanSecs = 3600
frozenTimePeriodInSecs = 2630000
maxTota1DataSizeMB = 650000
All other related indexes.conf settings are default values.
If the event timestamp was 3739283 seconds ago, will it be searchable?
A. Yes, only if the bucket is still hot.
B. No, because the index will have exceeded its maximum size.
C. Yes, only if the index size is also below 650000 MB.
D. No, because the event time is greater than the retention time.
Answer: D (LEAVE A REPLY)
Explanation
The correct answer is D. No, because the event time is greater than the retention time.
According to the Splunk documentation1, the frozenTimePeriodInSecs setting in indexes.conf determines how long Splunk software retains indexed data before deleting it or archiving it to a remote storage. The default value is 188697600 seconds, which is equivalent to six years. The setting can be overridden on a per-index basis.

In this case, the cat_facts index has a frozenTimePeriodInSecs setting of 2630000 seconds, which is equivalent to about 30 days. This means that any event that is older than 30 days from the current time will be removed from the index and will not be searchable.
The event timestamp was 3739283 seconds ago, which is equivalent to about 43 days. This means that the event is older than the retention time of the cat_facts index and will not be searchable.
The other settings in the stanza, such as maxHotSpanSecs and maxTota1DataSizeMB, do not affect the retention time of the events. They only affect the size and duration of the buckets that store the events.
References:1:Set a retirement and archiving policy - Splunk Documentation

NEW QUESTION: 68
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
Answer: (SHOW ANSWER)
Explanation/Reference:
https://answers.splunk.com/answers/558653/indexesconf-and-volume-settings.html

NEW QUESTION: 69
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: 70
Which of the following statements describe deployment management? (select all that apply)
A. Requires an Enterprise license
B. Is responsible for sending apps to forwarders.
C. Once used, is the only way to manage forwarders
D. Can automatically restart the host OS running the forwarder.
Answer: (SHOW ANSWER)
Explanation
https://docs.splunk.com/Documentation/Splunk/8.2.2/Admin/Distdeploylicenses#:~:text=License%20requiremen
"All Splunk Enterprise instances functioning as management components needs access to an Enterprise license. Management components include the deployment server, the indexer cluster manager node, the search head cluster deployer, and the monitoring console."
https://docs.splunk.com/Documentation/Splunk/8.2.2/Updating/Aboutdeploymentserver
"The deployment server is the tool for distributing configurations, apps, and content updates to groups of Splunk Enterprise instances."

NEW QUESTION: 71
Which Splunk indexer operating system platform is supported when sending logs from a Windows universal forwarder?
A. Linux platform only
B. Windows platform only.
C. None of the above.
D. Any OS platform
Answer: (SHOW ANSWER)

NEW QUESTION: 72
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

NEW QUESTION: 73
Which option on the Add Data menu is most useful for testing data ingestion without creating inputs.conf?
A. Upload option
B. Monitor option
C. Download option
D. Forward option
Answer: (SHOW ANSWER)

NEW QUESTION: 74
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: (SHOW ANSWER)
Explanation/Reference: https://docs.splunk.com/Documentation/Splunk/7.3.1/Admin/Configurationfiledirectories

NEW QUESTION: 75
An index stores its data in buckets. Which default directories does Splunk use to store buckets? (Choose all that apply.)
A. colddb
B. frozendb
C. bucketdb
D. db
Answer: A,D (LEAVE A REPLY)

NEW QUESTION: 76
A new forwarder has been installed with a manually created deploymentclient.conf.
What is the next step to enable the communication between the forwarder and the deployment server?
A. Restart Splunk on the deployment server.
B. Enable the deployment client in Splunk Web under Forwarder Management.
C. Restart Splunk on the deployment client.
D. Wait for up to the time set in the phoneHomeIntervalInSecs setting.
Answer: C (LEAVE A REPLY)
The next step to enable the communication between the forwarder and the deployment server after installing a new forwarder with a manually created deploymentclient.conf is to restart Splunk on the deployment client. The deploymentclient.conf file contains the settings for the deployment client, which is a Splunk instance that receives updates from the deployment server. The file must include the targetUri attribute, which specifies the hostname and management port of the deployment server. To apply the changes in the deploymentclient.conf file, Splunk must be restarted on the deployment client. Therefore, option C is the correct answer. Reference: Splunk Enterprise Certified Admin | Splunk, [Configure deployment clients - Splunk Documentation]

Valid SPLK-1003 Dumps shared by TrainingDump.com for Helping Passing SPLK-1003 Exam! TrainingDump.com now offer the **newest SPLK-1003 exam dumps**, the TrainingDump.com SPLK-1003 exam **questions have been updated** and **answers have been corrected** get the **newest** TrainingDump.com SPLK-1003 dumps with Test Engine here:
https://www.trainingdump.com/Splunk/SPLK-1003-practice-exam-dumps.html (**232** Q&As Dumps, **40%OFF** **Special Discount:** **Exam-Tests**)

NEW QUESTION: 77
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.
Answer: (SHOW ANSWER)
Explanation
https://docs.splunk.com/Documentation/Splunk/8.2.2/Data/UsetheHTTPEventCollector
"The HTTP Event Collector (HEC) lets you send data and application events to a Splunk deployment over the HTTP and Secure HTTP (HTTPS) protocols. HEC uses a token-based authentication model. You can generate a token and then configure a logging library or HTTP client with the token to send data to HEC in a specific format. This process eliminates the need for a Splunk forwarder when you send application events."

NEW QUESTION: 78
What are the required stanza attributes when configuring the transforms. conf to manipulate or remove events?
A. REGEX, DEST_KEY FORMATTING
B. REGEX, DEST. FORMAT
C. REGEX, DEST_KEY, FORMAT
D. REGEX. SRC_KEY, FORMAT
Answer: B (LEAVE A REPLY)

NEW QUESTION: 79
Which Splunk component does a search head primarily communicate with?
A. Indexer
B. Forwarder
C. Cluster master
D. Deployment server
Answer: A (LEAVE A REPLY)
Explanation/Reference: https://docs.splunk.com/Documentation/Splunk/7.3.1/InheritedDeployment/Deploymenttopology

NEW QUESTION: 80
Which Splunk forwarder has a built-in license?
A. Universal forwarder
B. Light forwarder
C. Cloud forwarder
D. Heavy forwarder
Answer: (SHOW ANSWER)

NEW QUESTION: 81
Which of the following Splunk components require a separate installation package?
A. License master
B. Universal forwarder
C. Deployment server
D. Heavy forwarder
Answer: (SHOW ANSWER)

NEW QUESTION: 82
Which of the following are reasons to create separate indexes? (Choose all that apply.)
A. File organization.
B. Restrict user permissions.
C. Increase number of users.
D. Different retention times.
Answer: A,D (LEAVE A REPLY)

NEW QUESTION: 83
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: 84
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: (SHOW ANSWER)
Explanation
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: 85
What is the valid option for a [monitor] stanza in inputs.conf?
A. enabled
B. datasource
C. server_name
D. ignoreOlderThan
Answer: (SHOW ANSWER)
Reference:
Monitorfilesanddirectorieswithinputs.conf

NEW QUESTION: 86
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: 87
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.conffile:
/opt/splunk/etc/deployment-apps/my_TA/local/inputs.conf
[monitor:///var/log/maillog]

sourcetype=maillog
index=syslog
Which file is now monitored?
/var/log/messages
A. /var/log/maillog
B. none of the above
C.
D. /var/log/maillogand /var/log/messages
Answer: D (LEAVE A REPLY)

NEW QUESTION: 88
What hardware attribute would need to be changed to increase the number of simultaneous searches (ad-hoc and scheduled) on a single search head?
A. Disk
B. CPUs
C. Memory
D. Network interface cards
Answer: B (LEAVE A REPLY)
https://docs.splunk.com/Documentation/Splunk/7.3.1/DistSearch/SHCarchitecture Scroll down to section titled, How the cluster handles concurrent search quotas, "Overall search quota. This quota determines the maximum number of historical searches (combined scheduled and ad hoc) that the cluster can run concurrently. This quota is configured with max_Searches_per_cpu and related settings in limits.conf."

NEW QUESTION: 89
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 number of warm buckets is reached.
D. When the maximum warm bucket size has been reached.
Answer: C (LEAVE A REPLY)

NEW QUESTION: 90
Which of the following authentication types requires scripting in Splunk?
A. ADFS
B. LDAP
C. SAML
D. RADIUS
Answer: D (LEAVE A REPLY)
Explanation
https://answers.splunk.com/answers/131127/scripted-authentication.html
Scripted Authentication: An option for Splunk Enterprise authentication. You can use an authentication system that you have in place (such as PAM or RADIUS) by configuringauthentication.conf to use a script instead of using LDAP or Splunk Enterprise default authentication.

NEW QUESTION: 91
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: (SHOW ANSWER)
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."

Valid SPLK-1003 Dumps shared by TrainingDump.com for Helping Passing SPLK-1003 Exam! TrainingDump.com now offer the **newest SPLK-1003 exam dumps**, the TrainingDump.com SPLK-1003 exam **questions have been updated** and **answers have been corrected** get the **newest** TrainingDump.com SPLK-1003 dumps with Test Engine here:
https://www.trainingdump.com/Splunk/SPLK-1003-practice-exam-dumps.html (**232** Q&As Dumps, **40%OFF** **Special Discount:** **Exam-Tests**)

NEW QUESTION: 92
The following stanzas in inputs. conf are currently being used by a deployment client:
[udp: //145.175.118.177:1001
Connection_host = dns
sourcetype = syslog
Which of the following statements is true of data that is received via this input?
A. If Splunk is restarted, data will be queued and then sent when Splunk has restarted.
B. Local firewall ports do not need to be opened on the deployment client since the port is defined in inputs.conf.
C. The host value associated with data received will be the IP address that sent the data.
D. If Splunk is restarted, data may be lost.
Answer: D (LEAVE A REPLY)
Explanation
This is because the input type is UDP, which is an unreliable protocol that does not guarantee delivery, order, or integrity of the data packets. UDP does not have any mechanism to resend or acknowledge the data packets, so if Splunk is restarted, any data that was in transit or in the buffer may be dropped and not indexed.

NEW QUESTION: 93
Where are deployment server apps mapped to clients?
A. Client Applications tab in forwarder management interface or clientapps.conf.
B. Server Classes tab in forwarder management interface or serverclass.conf.
C. Clients tab in forwarder management interface or deploymentclient.conf.
D. Apps tab in forwarder management interface or clientapps.conf.
Answer: B (LEAVE A REPLY)

NEW QUESTION: 94
What is the correct example to redact a plain-text password from raw events?

A. in props.conf:
[identity]
REGEX-redact_pw = s/password=([^,|/s]+)/ ####REACTED####/g
B. in props.conf:
[identity]
SEDCMD-redact_pw = s/password=([^,|/s]+)/ ####REACTED####/g
C. in transforms.conf:
[identity]
SEDCMD-redact_pw = s/password=([^,|/s]+)/ ####REACTED####/g
D. in transforms.conf:
[identity]
REGEX-redact_pw = s/password=([^,|/s]+)/ ####REACTED####/g
Answer: B (LEAVE A REPLY)
The correct answer is B. in props.conf:
[identity]
SEDCMD-redact_pw = s/password=([^,|/s]+)/ ####REACTED####/g
According to the Splunk documentation1, to redact sensitive data from raw events, you need to use the SEDCMD attribute in the props.conf file. The SEDCMD attribute applies a sed expression to the raw data before indexing. The sed expression can use the s command to replace a pattern with a substitution string. For example, the following sed expression replaces any occurrence of password= followed by any characters until a comma, whitespace, or slash with ####REACTED####:
s/password=([^,|/s]+)/ ####REACTED####/g
The g flag at the end means that the replacement is applied globally, not just to the first match.
Option A is incorrect because it uses the REGEX attribute instead of the SEDCMD attribute. The REGEX attribute is used to extract fields from events, not to modify them.
Option C is incorrect because it uses the transforms.conf file instead of the props.conf file. The transforms.conf file is used to define transformations that can be applied to fields or events, such as lookups, evaluations, or replacements. However, these transformations are applied after indexing, not before.
Option D is incorrect because it uses both the wrong attribute and the wrong file. There is no REGEX-redact_pw attribute in the transforms.conf file.

NEW QUESTION: 95
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. A list of the current running props, conf configurations along with a file path from which the configuration was made
C. list of all the configurations on-disk that Splunk contains.
D. A list of props. conf configurations as they are on-disk along with a file path from which the configuration is located
Answer: D (LEAVE A REPLY)

NEW QUESTION: 96
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)
Explanation
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: 97
Which layers are involved in Splunk configuration file layering? (Choose all that apply.)
A. Global context
B. User context
C. Forwarder context
D. App context
Answer: A,B,D (LEAVE A REPLY)

NEW QUESTION: 98
In which Splunk configuration is the SEDCMD used?
A. props, conf
B. inputs.conf
C. indexes.conf
D. transforms.conf
Answer: (SHOW ANSWER)
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: 99
Which of the following apply to how distributed search works? (select all that apply)
A. The search peers pull the data from the forwarders.
B. The search head dispatches searches to the peers
C. Peers run searches in parallel and return their portion of results.
D. The search head consolidates the individual results and prepares reports
Answer: B,C,D (LEAVE A REPLY)

NEW QUESTION: 100
A Splunk administrator has been tasked with developing a retention strategy to have frequently accessed data sets on SSD storage and to have older, less frequently accessed data on slower NAS storage. They have set a mount point for the NAS. Which parameter do they need to modify to set the path for the older, less frequently accessed data in indexes.conf?
A. homepath
B. thawedPath
C. summaryHomePath
D. colddeath
Answer: D (LEAVE A REPLY)
The coldPath parameter defines the path for the cold buckets, which are the oldest and least frequently accessed data in an index1. By setting the coldPath to point to the NAS mount point, the Splunk administrator can achieve the retention strategy of having older data on slower NAS storage.

NEW QUESTION: 101
The Splunk administrator wants to ensure data is distributed evenly amongst the indexers. To do this, he runs the following search over the last 24 hours:
index=*
What field can the administrator check to see the data distribution?
A. host
B. index
C. linecount
D. splunk_server
Answer: D (LEAVE A REPLY)
Explanation
https://docs.splunk.com/Documentation/Splunk/8.2.2/Knowledge/Usedefaultfields splunk_server The splunk server field contains the name of the Splunk server containing the event. Useful in a distributed Splunk environment. Example: Restrict a search to the main index on a server named remote.
splunk_server=remote index=main 404

NEW QUESTION: 102
Which of the following must be done to define user permissions when integrating Splunk with LDAP?
A. Map Users
B. Map Groups
C. Map LDAP Inheritance
D. Map LDAP to Active Directory
Answer: B (LEAVE A REPLY)
Explanation
https://docs.splunk.com/Documentation/Splunk/8.1.3/Security/ConfigureLDAPwithSplunkWeb
"You can map either users or groups, but not both. If you are using groups, all users must be members of an appropriate group. Groups inherit capabilities form the highest level role they're a member of." "If your LDAP environment does not have group entries, you can treat each user as its own group."

NEW QUESTION: 103
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
Answer: (SHOW ANSWER)
https://docs.splunk.com/Splexicon:Searchpeer
"A Splunk platform instance that responses to search requests from a search head. The term "Search peer" is usually synonymous with the indexer role in a distributed search topology..."

NEW QUESTION: 104
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.
Answer: D (LEAVE A REPLY)
Explanation
https://docs.splunk.com/Documentation/Splunk/8.2.2/Updating/Aboutdeploymentserver
"The deployment server is the tool for distributing configurations, apps, and content updates to groups of Splunk Enterprise instances."

NEW QUESTION: 105
When running the command shown below, what is the default path in which deployment server. conf is created?
splunk set deploy-poll deployServer:port
A. SFLUNK_HOME/etc/deployment
B. SPLUNK_HOME/etc/system/local
C. SPLUNK_HOME/etc/system/default
D. SPLUNK_KOME/etc/apps/deployment
Answer: (SHOW ANSWER)
https://docs.splunk.com/Documentation/Splunk/8.1.1/Updating/Definedeploymentclasses#Ways_to_define_server_classes "When you use forwarder management to create a new server class, it saves the server class definition in a copy of serverclass.conf under $SPLUNK_HOME/etc/system/local. If, instead of using forwarder management, you decide to directly edit serverclass.conf, it is recommended that you create the serverclass.conf file in that same directory, $SPLUNK_HOME/etc/system/local."

NEW QUESTION: 106
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

Valid SPLK-1003 Dumps shared by TrainingDump.com for Helping Passing SPLK-1003 Exam! TrainingDump.com now offer the **newest SPLK-1003 exam dumps**, the TrainingDump.com SPLK-1003 exam **questions have been updated** and **answers have been corrected** get the **newest** TrainingDump.com SPLK-1003 dumps with Test Engine here:
https://www.trainingdump.com/Splunk/SPLK-1003-practice-exam-dumps.html (**232** Q&As Dumps, **40%OFF** **Special Discount:** **Exam-Tests**)

NEW QUESTION: 107
A Splunk administrator has been tasked with developing a retention strategy to have frequently accessed data sets on SSD storage and to have older, less frequently accessed data on slower NAS storage. They have set a mount point for the NAS. Which parameter do they need to modify to set the path for the older, less frequently accessed data in indexes.conf?
A. thawedPath
B. colddeath
C. homepath
D. summaryHomePath

Answer: B (LEAVE A REPLY)
Explanation
The coldPath parameter defines the path for the cold buckets, which are the oldest and least frequently accessed data in an index1. By setting the coldPath to point to the NAS mount point, the Splunk administrator can achieve the retention strategy of having older data on slower NAS storage.

NEW QUESTION: 108
In this example, if useACK is set to true and the maxQueueSize is set to 7MB, what is the size of the wait queue on this universal forwarder?
A. 21MB
B. 14MB
C. 7MB
D. 28MB
Answer: (SHOW ANSWER)

NEW QUESTION: 109
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: B (LEAVE A REPLY)
Explanation
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: 110
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: (SHOW ANSWER)
Explanation
https://docs.splunk.com/Documentation/Splunk/8.1.0/Data/ConsiderationsfordecidinghowtomonitorWindowsdat
"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: 111
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)
https://docs.splunk.com/Documentation/Splunk/latest/Indexer/Setaretirementandarchivingpolicy

NEW QUESTION: 112
When using a directory monitor input, specific source type can be selectively overridden using which configuration file?
A. props.conf
B. sourcetypes.conf
C. transforms.conf
D. outputs.conf
Answer: (SHOW ANSWER)
Reference:
When using a directory monitor input, specific source types can be selectively overridden using props.conf. The props.conf file contains settings for parsing and indexing data, as well as search-time field extractions. The props.conf file can be used to assign or change source types for specific inputs using the sourcetype attribute. Therefore, option A is the correct answer. Reference: Splunk Enterprise Certified Admin | Splunk, [Configure directory monitor inputs - Splunk Documentation]

NEW QUESTION: 113
Which forwarder type can parse data prior to forwarding?
A. Heaviest forwarder
B. Heavy forwarder
C. Hyper forwarder
D. Universal forwarder
Answer: B (LEAVE A REPLY)

NEW QUESTION: 114
Event processing occurs at which phase of the data pipeline?
A. Search
B. Indexing
C. Parsing
D. Input
Answer: C (LEAVE A REPLY)
According to the Splunk documentation1, event processing occurs at the parsing phase of the data pipeline. The parsing phase is where Splunk software processes incoming data into individual events, extracts timestamp information, assigns source types, and performs other tasks to make the data searchable1. The parsing phase can also apply field extractions, event type matching, and other transformations to the events2.

NEW QUESTION: 115
During search time, which directory of configuration files has the highest precedence?
A. $SPLUNK HCME/etc/users/admin/local
B. $SPLUNK_HCME/etc/apps/app1/local
C. $SFLUNK_KOME/etc/system/local

D. $SPLUNK_KCME/etc/system/default
Answer: C (LEAVE A REPLY)

NEW QUESTION: 116
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 C
B. Option B
C. Option D
D. option A
Answer: C (LEAVE A REPLY)

NEW QUESTION: 117
A security team needs to ingest a static file for a specific incident. The log file has not been collected previously and future updates to the file must not be indexed.
Which command would meet these needs?
A. splunk add one shot / opt/ incident [data .log -index incident
B. splunk edit monitor /opt/incident/data.* -index incident
C. splunk add monitor /opt/incident/data.log -index incident
D. splunk edit oneshot [opt/ incident/data.* -index incident
Answer: A (LEAVE A REPLY)
Explanation
The correct answer is A. splunk add one shot / opt/ incident [data . log -index incident According to the Splunk documentation1, the splunk add one shot command adds a single file or directory to the Splunk index and then stops monitoring it. This is useful for ingesting static files that do not change or update. The command takes the following syntax:
splunk add one shot <file> -index <index_name>
The file parameter specifies the path to the file or directory to be indexed. The index parameter specifies the name of the index where the data will be stored. If the index does not exist, Splunk will create it automatically.

Option B is incorrect because the splunk edit monitor command modifies an existing monitor input, which is used for ingesting files or directories that change or update over time. This command does not create a new monitor input, nor does it stop monitoring after indexing.
Option C is incorrect because the splunk add monitor command creates a new monitor input, which is also used for ingesting files or directories that change or update over time. This command does not stop monitoring after indexing.
Option D is incorrect because the splunk edit oneshot command does not exist. There is no such command in the Splunk CLI.
References:1:Monitor files and directories with inputs.conf - Splunk Documentation

NEW QUESTION: 118
In which Splunk configuration is the SEDCMDused?
A. props.conf
B. inputs.conf
C. indexes.conf
D. transforms.conf
Answer: A (LEAVE A REPLY)
Explanation
Explanation/Reference: https://answers.splunk.com/answers/212128/why-sedcmd-configured-in-propsconf-is-working- duri.html

NEW QUESTION: 119
How is data handled by Splunk during the input phase of the data ingestion process?
A. Data is treated as streams.
B. Data is broken up into events.
C. Data is initially written to disk.
D. Data is measured by the license meter.
Answer: (SHOW ANSWER)
Explanation/Reference: https://docs.splunk.com/Documentation/Splunk/8.0.5/Deploy/Datapipeline

NEW QUESTION: 120
Which of the following must be done to define user permissions when integrating Splunk with LDAP?
A. Map LDAP Inheritance
B. Map LDAP to Active Directory
C. Map Groups
D. Map Users
Answer: C (LEAVE A REPLY)

NEW QUESTION: 121
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: (SHOW ANSWER)

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

Valid SPLK-1003 Dumps shared by TrainingDump.com for Helping Passing SPLK-1003 Exam! TrainingDump.com now offer the **newest SPLK-1003 exam dumps**, the TrainingDump.com SPLK-1003 exam **questions have been updated** and **answers have been corrected** get the **newest** TrainingDump.com SPLK-1003 dumps with Test Engine here:
https://www.trainingdump.com/Splunk/SPLK-1003-practice-exam-dumps.html (**232** Q&As Dumps, **40%OFF** **Special Discount:** **Exam-Tests**)

NEW QUESTION: 122
What is the correct order of steps in Duo Multifactor Authentication?
A. 1. Request Login
2. Connect to SAML server
3 Duo MFA
4 Create User session
5 Authentication Granted 6. Log into Splunk
B. 1. Request Login 2 Duo MFA
3. Authentication Granted 4 Connect to SAML server
5. Log into Splunk
6. Create User session
C. 1 Request Login
2 Check authentication / group mapping
3 Authentication Granted
4. Duo MFA
5. Create User session
6. Log into Splunk
D. 1 Request Login 2 Duo MFA
3. Check authentication / group mapping
4 Create User session
5. Authentication Granted
6 Log into Splunk
Answer: (SHOW ANSWER)
Using the provided DUO/Splunk reference URL https://duo.com/docs/splunk Scroll down to the Network Diagram section and note the following 6 similar steps
1 - SPlunk connection initiated
2 - Primary authentication
3 - Splunk connection established to Duo Security over TCP port 443
4 - Secondary authentication via Duo Security's service
5 - Splunk receives authentication response
6 - Splunk session logged in.

NEW QUESTION: 123
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.
Answer: B (LEAVE A REPLY)
Explanation/Reference: http://dev.splunk.com/view/event-collector/SP-CAAAE6M

NEW QUESTION: 124
All search-time field extractions should be specified on which Splunk component?
A. Indexer
B. Universal forwarder
C. Search head
D. Deployment server
Answer: A (LEAVE A REPLY)

NEW QUESTION: 125
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: 126
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
Answer: D (LEAVE A REPLY)
Explanation/Reference: https://docs.splunk.com/Documentation/Splunk/8.0.5/Updating/Updateconfigurations

NEW QUESTION: 127
Immediately after installation, what will a Universal Forwarder do first?
A. Automatically detect any indexers in its subnet and begin routing data.
B. Begin reading local files on its server.
C. Begin generating internal Splunk logs.
D. Send an email to the operator that the installation process has completed.

Answer: C (LEAVE A REPLY)
Explanation
Begin generating internal Splunk logs. Immediately after installation, a Universal Forwarder will start generating internal Splunk logs that contain information about its own operation, such as startup and shutdown events, configuration changes, data ingestion, and forwarding activities1. These logs are stored in the $SPLUNK_HOME/var/log/splunk directory on the Universal Forwarder machine2.

NEW QUESTION: 128
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.
Answer: (SHOW ANSWER)
Explanation/Reference: https://docs.splunk.com/Documentation/Splunk/7.2.6/Security/Aboutusersandroles

NEW QUESTION: 129
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
Answer: C (LEAVE A REPLY)
Explanation
Indexers, search head, deployment server, license master, universal forwarder. This is the combination of Splunk component instances that are needed to handle the volume of data from collecting log files from 50 Linux servers and 200 Windows servers, following the best practices. The roles and functions of these components are:
* Indexers: These are the Splunk instances that index the data and make it searchable. They also perform some data processing, such as timestamp extraction, line breaking, and field extraction. Multiple indexers can be clustered together to provide high availability, data replication, and load balancing.
* Search head: This is the Splunk instance that coordinates the search across the indexers and merges the results from them. It also provides the user interface for searching, reporting, and dashboarding. A search head can also be clustered with other search heads to provide high availability, scalability, and load balancing.
* Deployment server: This is the Splunk instance that manages the configuration and app deployment for
* the universal forwarders. It allows the administrator to centrally control the inputs.conf, outputs.conf, and other configuration files for the forwarders, as well as distribute apps and updates to them.
* License master: This is the Splunk instance that manages the licensing for the entire Splunk deployment.
It tracks the license usage of all the Splunk instances and enforces the license limits and violations. It also allows the administrator to add, remove, or change licenses.
* Universal forwarder: These are the lightweight Splunk instances that collect data from various sources and forward it to the indexers or other forwarders. They do not index or parse the data, but only perform minimal processing, such as compression and encryption. They are installed on the Linux and Windows servers that generate the log files.

NEW QUESTION: 130
Which of the following types of data count against the license daily quota?
A. Replicated data

B. splunkd logs
C. Summary index data
D. Windows internal logs
Answer: D (LEAVE A REPLY)
https://docs.splunk.com/Documentation/Splunk/8.0.3/Admin/Distdeploylicenses#Clustered_deployments_and_licensing_issues

NEW QUESTION: 131
The following stanza is active in indexes.conf:
[cat_facts]
maxHotSpanSecs = 3600
frozenTimePeriodInSecs = 2630000
maxTota1DataSizeMB = 650000
All other related indexes.conf settings are default values.
If the event timestamp was 3739283 seconds ago, will it be searchable?
A. Yes, only if the bucket is still hot.
B. No, because the index will have exceeded its maximum size.
C. Yes, only if the index size is also below 650000 MB.
D. No, because the event time is greater than the retention time.
Answer: (SHOW ANSWER)
The correct answer is D. No, because the event time is greater than the retention time.
According to the Splunk documentation1, the frozenTimePeriodInSecs setting in indexes.conf determines how long Splunk software retains indexed data before deleting it or archiving it to a remote storage. The default value is 188697600 seconds, which is equivalent to six years. The setting can be overridden on a per-index basis.
In this case, the cat_facts index has a frozenTimePeriodInSecs setting of 2630000 seconds, which is equivalent to about 30 days. This means that any event that is older than 30 days from the current time will be removed from the index and will not be searchable.
The event timestamp was 3739283 seconds ago, which is equivalent to about 43 days. This means that the event is older than the retention time of the cat_facts index and will not be searchable.
The other settings in the stanza, such as maxHotSpanSecs and maxTota1DataSizeMB, do not affect the retention time of the events. They only affect the size and duration of the buckets that store the events.

NEW QUESTION: 132
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: (SHOW ANSWER)
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: 133
Which of the following statements apply to directory inputs? {select all that apply)
A. When adding new log files to a monitored directory, the forwarder must be restarted to take them into account.
B. All discovered text files are consumed.
C. Compressed files are ignored by default
D. Splunk recursively traverses through the directory structure.
Answer: B,D (LEAVE A REPLY)

NEW QUESTION: 134
Which of the following is valid distribute search group?
A)
```
[distributedSearch:Paris]
default = false
servers = server1, server2
```
B)
```
[searchGroup:Paris]
default = false
servers = server1:8089, server2:8089
```
C)
```
[searchGroup:Paris]
default = false
servers = server1:9997, server2:9997
```
D)
```
[distributedSearch:Paris]
default = false
servers = server1:8089, server2:8089
```
A. option A
B. Option B
C. Option C
D. Option D
Answer: D (LEAVE A REPLY)

NEW QUESTION: 135
With authentication methods are natively supported within Splunk Enterprise? (Select all that apply.)
A. LDAP
B. SAML
C. RADIUS
D. Duo Multifactor Authentication
Answer: A,D (LEAVE A REPLY)
Explanation/Reference: https://docs.splunk.com/Documentation/Splunk/7.3.1/Security/SetupuserauthenticationwithSplunk

NEW QUESTION: 136
A Universal Forwarder is collecting two separate sources of data (A,B). Source A is being routed through a Heavy Forwarder and then to an indexer. Source B is being routed directly to the indexer. Both sets of data require the masking of raw text strings before being written to disk. What does the administrator need to do to ensure that the masking takes place successfully?
A. Make sure that props . conf and transforms . conf are both present on the in-dexer and the search head.
B. For source A, make sure that props . conf is in place on the indexer; and for source B, make sure transforms . conf is present on the Heavy Forwarder.
C. Make sure that props . conf and transforms . conf are both present on the Universal Forwarder.
D. Place both props . conf and transforms . conf on the Heavy Forwarder for source A, and place both props . conf and transforms . conf on the indexer for source B.
Answer: D (LEAVE A REPLY)
Explanation
The correct answer is D. Place both props . conf and transforms . conf on the Heavy Forwarder for source A, and place both props . conf and transforms . conf on the indexer for source B.
According to the Splunk documentation1, to mask sensitive data from raw events, you need to use the SEDCMD attribute in the props.conf file and the REGEX attribute in the transforms.conf file. The SEDCMD attribute applies a sed expression to the raw data before indexing, while the REGEX attribute defines a regular expression to match the data to be masked. You need to place these files on the Splunk instance that parses the data, which is usually the indexer or the heavy forwarder2. The universal forwarder does not parse the data, so it does not need these files.
For source A, the data is routed through a heavy forwarder, which can parse the data before sending it to the indexer. Therefore, you need to place both props.conf and transforms.conf on the heavy forwarder for source A, so that the masking takes place before indexing.
For source B, the data is routed directly to the indexer, which parses and indexes the data. Therefore, you need to place both props.conf and transforms.conf on the indexer for source B, so that the masking takes place before indexing.
References: 1: Redact data from events - Splunk Documentation 2: Where do I configure my Splunk settings?
- Splunk Documentation

Valid SPLK-1003 Dumps shared by TrainingDump.com for Helping Passing SPLK-1003 Exam! TrainingDump.com now offer the **newest SPLK-1003 exam dumps**, the TrainingDump.com SPLK-1003 exam **questions have been updated** and **answers have been corrected** get the **newest** TrainingDump.com SPLK-1003 dumps with Test Engine here:
https://www.trainingdump.com/Splunk/SPLK-1003-practice-exam-dumps.html (**232** Q&As Dumps, **40%OFF** **Special Discount:** **Exam-Tests**)

NEW QUESTION: 137
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, deployment server, universal forwarders
C. Indexers, search head, deployment server, license master, universal forwarder
D. Indexers, search head, universal forwarders, license master
Answer: C (LEAVE A REPLY)

NEW QUESTION: 138
Which data pipeline phase is the last opportunity for defining event boundaries?
A. Input phase
B. Indexing phase
C. Parsing phase
D. Search phase

Answer: (SHOW ANSWER)
Explanation
Reference
https://docs.splunk.com/Documentation/Splunk/8.2.3/Admin/Configurationparametersandthedatapipeline The parsing phase is the process of extracting fields and values from raw data. The parsing phase respects LINE_BREAKER, SHOULD_LINEMERGE, BREAK_ONLY_BEFORE_DATE, and all other line merging settings in props.conf. These settings determine how Splunk breaks the data into events based on certain criteria, such as timestamps or regular expressions. The event boundaries are defined by the props.conf file, which can be modified by the administrator. Therefore, the parsing phase is the last opportunity for defining event boundaries.

NEW QUESTION: 139
Which of the following is accurate regarding the input phase?
A. Breaks data into events with timestamps.
B. Applies event-level transformations.
C. Fine-tunes metadata.
D. Performs character encoding.
Answer: D (LEAVE A REPLY)
Explanation
https://docs.splunk.com/Documentation/Splunk/latest/Deploy/Datapipeline "The data pipeline segments in depth. INPUT - In the input segment, Splunk software consumes data. It acquires the raw data stream from its source, breaks it into 64K blocks, and annotates each block with some metadata keys. The keys can also include values that are used internally, such as the character encoding of the data stream, and values that control later processing of the data, such as the index into which the events should be stored. PARSING Annotating individual events with metadata copied from the source-wide keys. Transforming event data and metadata according to regex transform rules."

NEW QUESTION: 140
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
Answer: (SHOW ANSWER)
Explanation
Explanation/Reference: http://dev.splunk.com/view/dev-guide/SP-CAAAE3A

NEW QUESTION: 141
Which of the following are supported options when configuring optional network inputs?
A. Metadata override, sender filtering options, network input queues (quantum queues)
B. Metadata override, sender filtering options, network input queues (memory/persistent queues)
C. Filename override, sender filtering options, network output queues (memory/persistent queues)
D. Metadata override, receiver filtering options, network input queues (memory/persistent queues)
Answer: B (LEAVE A REPLY)
https://docs.splunk.com/Documentation/Splunk/latest/Data/Monitornetworkports

NEW QUESTION: 142

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

NEW QUESTION: 143
The Splunk administrator wants to ensure data is distributed evenly amongst the indexers. To do this, he runs the following search over the last 24 hours:
index=*
What field can the administrator check to see the data distribution?
A. host
B. index
C. linecount
D. splunk_server
Answer: D (LEAVE A REPLY)
https://docs.splunk.com/Documentation/Splunk/8.2.2/Knowledge/Usedefaultfields splunk_server The splunk server field contains the name of the Splunk server containing the event. Useful in a distributed Splunk environment. Example: Restrict a search to the main index on a server named remote. splunk_server=remote index=main 404

NEW QUESTION: 144
Local user accounts created in Splunk store passwords in which file?
A. $ SFLUNK_HOME/etc/passwd
B. $ SFLUNK_HOME/etc/authentication
C. $ S?LUNK_HOME/etc/users/passwd.conf
D. $ SPLUNK HOME/etc/users/authentication.conf
Answer: (SHOW ANSWER)
Per the provided reference URL https://docs.splunk.com/Documentation/Splunk/7.3.1/Admin/User-seedconf
"To set the default username and password, place user-seed.conf in $SPLUNK_HOME/etc/system/local. You must restart Splunk to enable configurations. If the $SPLUNK_HOME/etc/passwd file is present, the settings in this file (user-seed.conf) are not used."

NEW QUESTION: 145
An admin oversees an environment with a 1000 GBI day license. The configuration file server.conf has strict pool quota=false set. The license is divided into the following three pools, and today's usage is shown on the right-hand column:
Pool License Size Today's usage
X 500 GB/day 100 GB
Y 350 GB/day 400 GB
Z 150 GB/day 300 GB
Given this, which pool(s) are issued warnings?
A. All pools
B. Z only
C. None

D. Y and Z

Answer: D (LEAVE A REPLY)

In Splunk Enterprise, when you configure the server.conf file with strict pool quota=false, it means that license pools are allowed to share the total available license quota rather than being restricted to their individually allocated quotas. However, this does not prevent pools from issuing warnings if they exceed their allocated limits.

Given the environment with a 1000 GB/day license split into three pools:

Pool X: 500 GB/day license, 100 GB used

Pool Y: 350 GB/day license, 400 GB used

Pool Z: 150 GB/day license, 300 GB used

Let's analyze the usage:

Pool X is allocated 500 GB/day but has only used 100 GB, well within its limit.

Pool Y is allocated 350 GB/day but has used 400 GB, which exceeds its limit by 50 GB.

Pool Z is allocated 150 GB/day but has used 300 GB, which exceeds its limit by 150 GB.

Even with strict pool quota=false, pools Y and Z have exceeded their individual allocated quotas and will issue warnings. Pool X has not exceeded its quota and thus will not issue any warnings.

Therefore, the pools that are issued warnings are Y and Z.

NEW QUESTION: 146

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

B. /var/log/maillog and /var/log/messages

C. /var/log/messages

D. none of the above

Answer: A (LEAVE A REPLY)

NEW QUESTION: 147

In this source definition the MAX_TIMESTAMP_LOOKHEAD is missing. Which value would fit best?



Event example:

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

A. MAX_TIMESTAMP_L0CKAHEAD = 5

B. MAX_TIMESTAMP_LOOKAHEAD - 10

C. MAX_TIMESTAMF_LOOKHEAD = 20

D. MAX TIMESTAMP LOOKAHEAD - 30

Answer: D (LEAVE A REPLY)

Explanation

https://docs.splunk.com/Documentation/Splunk/6.2.0/Data/Configuretimestamprecognition

"Specify how far (how many characters) into an event Splunk software should look for a timestamp." since TIME_PREFIX = ^ and timestamp is from 0-29 position, so D=30 will pick up the WHOLE timestamp correctly.

NEW QUESTION: 148

Given a forwarder with the following outputs.conf configuration:

[tcpout : mypartner]

Server = 145.188.183.184:9097

[tcpout : hfbank]

server = inputsl . mysplunkhfs . corp : 9997 , inputs2 . mysplunkhfs . corp : 9997 Which of the following is a true statement?

A. Data will continue to flow to hfbank if 145.1 g a) 183.184 : 9097 is unreachable.

B. Data is not encrypted to mypartner because 145.188 .183.184 : 9097 is specified by IP.

C. Data is encrypted to mypartner because 145.183.184 : 9097 is specified by IP.

D. Data will eventually stop flowing everywhere if 145.188.183.184 : 9097 is unreachable.

Answer: A (LEAVE A REPLY)

The outputs.conf file defines how forwarders send data to receivers1. You can specify some output configurations at installation time (Windows universal forwarders only) or the CLI, but most advanced configuration settings require that you edit outputs.conf1.

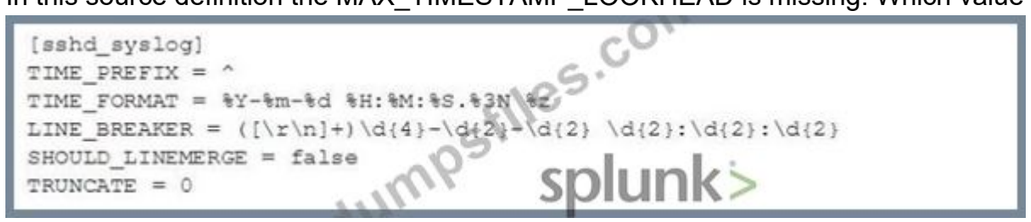
The [tcpout:...] stanza specifies a group of forwarding targets that receive data over TCP2. You can define multiple groups with different names and settings2.

The server setting lists one or more receiving hosts for the group, separated by commas2. If you specify multiple hosts, the forwarder load balances the data across them2.

Therefore, option A is correct, because the forwarder will send data to both inputsl.mysplunkhfs.corp:9997 and inputs2.mysplunkhfs.corp:9997, even if 145.188.183.184:9097 is unreachable.

NEW QUESTION: 149

In this source definition the MAX_TIMESTAMP_LOOKHEAD is missing. Which value would fit best?



Event example:

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

A. MAX_TIMESTAMP_L0CKAHEAD = 5
B. MAX_TIMESTAMP_LOOKAHEAD - 10
C. MAX_TIMESTAMF_LOOKHEAD = 20
D. MAX TIMESTAMP LOOKAHEAD - 30
Answer: D (LEAVE A REPLY)
https://docs.splunk.com/Documentation/Splunk/6.2.0/Data/Configuretimestamprecognition
"Specify how far (how many characters) into an event Splunk software should look for a timestamp." since TIME_PREFIX = ^ and timestamp is from 0-29 position, so D=30 will pick up the WHOLE timestamp correctly.

NEW QUESTION: 150
How can native authentication be disabled in Splunk?
A. Remove the $SPLUNK_HOME/etc/passwdfile
B. Create an empty $SPLUNK_HOME/etc/passwdfile
C. Set SPLUNK_AUTHENTICATION=falsein splunk-launch.conf
D. Set nativeAuthentication=falsein authentication.conf
Answer: A (LEAVE A REPLY)
Explanation/Reference: https://docs.splunk.com/Documentation/Splunk/8.0.5/Security/Secureyouradminaccount

NEW QUESTION: 151
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 Check authentication / group mapping
3 Authentication Granted
4. Duo MFA
5. Create User session
6. Log into Splunk
C. 1 Request Login 2 Duo MFA
3. Check authentication / group mapping
4 Create User session
5. Authentication Granted
6 Log into Splunk
D. 1. Request Login 2 Duo MFA
3. Authentication Granted 4 Connect to SAML server
5. Log into Splunk

6. Create User session
Answer: (SHOW ANSWER)

Valid SPLK-1003 Dumps shared by TrainingDump.com for Helping Passing SPLK-1003 Exam! TrainingDump.com now offer the **newest SPLK-1003 exam dumps**, the TrainingDump.com SPLK-1003 exam **questions have been updated** and **answers have been corrected** get the **newest** TrainingDump.com SPLK-1003 dumps with Test Engine here:
https://www.trainingdump.com/Splunk/SPLK-1003-practice-exam-dumps.html (**232** Q&As Dumps, **40%OFF** **Special Discount:** **Exam-Tests**)

NEW QUESTION: 152
A configuration file in a deployed app needs to be directly edited. Which steps would ensure a successful deployment to clients?
A. Make the change in $SPLUNK HOME/etc/dep10yment apps/$appName/10ca1/ on the deployment server, and the change will be automatically sent to the deployment clients.
B. Make the change in $SPLUNK HOME /etc/apps/$appname/local/ on any of the deployment clients, and then run the command . / splunk reload deploy-server to push that change to the deployment server.
C. Make the change in $SPLUNK HOME/etc/dep10yment apps/$appName/10ca1/ on the deployment server, and then run $SPLUNK HOME/bin/sp1unk reload deploy-server.
D. Make the change in $SPLUNK HOME/etc/apps/$appName/defau1t on the deployment server, and it will be distributed down to the clients' own local versions.
Answer: C (LEAVE A REPLY)
According to the Splunk documentation1, to customize a configuration file, you need to create a new file with the same name in a local or app directory. Then, add the specific settings that you want to customize to the local configuration file. Never change or copy the configuration files in the default directory. The files in the default directory must remain intact and in their original location. The Splunk Enterprise upgrade process overwrites the default directory.
To deploy configuration files to deployment clients, you need to use the deployment server. The deployment server is a Splunk Enterprise instance that distributes content and updates to deployment clients2. The deployment server uses a directory called $SPLUNK_HOME/etc/deployment-apps to store the apps and configuration files that it deploys to clients2. To update the configuration files in this directory, you need to edit them manually and then run the command $SPLUNK_HOME/bin/sp1unk reload deploy-server to make the changes take effect2.
Therefore, option A is incorrect because it does not include the reload command. Option B is incorrect because it makes the change on a deployment client instead of the deployment server. Option D is incorrect because it changes the default directory instead of the local directory.

NEW QUESTION: 153
Which forwarder type can parse data prior to forwarding?
A. Universal forwarder
B. Heaviest forwarder
C. Hyper forwarder
D. Heavy forwarder
Answer: D (LEAVE A REPLY)
Explanation/Reference: https://docs.splunk.com/Documentation/Splunk/7.3.1/Forwarding/Typesofforwarders

NEW QUESTION: 154
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: D (LEAVE A REPLY)
https://docs.splunk.com/Documentation/Splunk/8.1.1/Data/Monitornetworkports
Reference: Bypassautomaticsourcetypeassignment

NEW QUESTION: 155
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)
Explanation/Reference: https://docs.splunk.com/Documentation/Splunk/8.0.5/Updating/ Updateconfigurations#2._Reload_the_deployment_server

NEW QUESTION: 156
Where are license files stored?
A. $SPLUNK_HOME/etc/secure
B. $SPLUNK_HOME/etc/system
C. $SPLUNK_HOME/etc/licenses
D. $SPLUNK_HOME/etc/apps/licenses
Answer: C (LEAVE A REPLY)
Explanation/Reference: https://docs.splunk.com/Documentation/Splunk/7.3.1/Admin/LicenserCLIcommands

NEW QUESTION: 157
When would the following command be used?

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

A. To verify' the integrity of a local index.
B. To verify the integrity of a SmartStore index.
C. To verify the integrity of a SmartStore bucket.
D. To verify the integrity of a local bucket.
Answer: D (LEAVE A REPLY)
Explanation
To verify the integrity of a local bucket. The command ./splunk check-integrity -bucketPath [bucket path]

[-verbose] is used to verify the integrity of a local bucket by comparing the hashes stored in the l1Hashes and l2Hash files with the actual data in the bucket1. This command can help detect any tampering or corruption of the data.

NEW QUESTION: 158
How does the Monitoring Console monitor forwarders?
A. With internal logs forwarded by deployment server.
B. By pulling internal logs from forwarders.
C. With internal logs forwarded by forwarders.
D. By using the forwarder monitoring add-on
Answer: (SHOW ANSWER)

NEW QUESTION: 159
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.
Answer: A (LEAVE A REPLY)
Reference:
AboutsecuringyourSplunkconfigurationwithSSL

NEW QUESTION: 160
For single line event sourcetypes. it is most efficient to set SHOULD_linemerge to what value?
A. True
B. False
C. <regex string>
D. Newline Character
Answer: B (LEAVE A REPLY)
https://docs.splunk.com/Documentation/Splunk/latest/Data/Configureeventlinebreaking Attribute : SHOULD_LINEMERGE = [true|false] Description : When set to true, the Splunk platform combines several input lines into a single event, with configuration based on the settings described in the next section.

NEW QUESTION: 161
Within props. conf, which stanzas are valid for data modification? (select all that apply)
A. Host
B. Server
C. Sourcetype
D. Source
Answer: (SHOW ANSWER)

NEW QUESTION: 162
You update a props. conf file while Splunk is running. You do not restart Splunk and you run this command:

splunk btoo1 props list -debug. What will the output be?
A. list of all the configurations on-disk that Splunk contains.
B. A verbose list of all configurations as they were when splunkd started.
C. A list of props. conf configurations as they are on-disk along with a file path from which the configuration is located
D. A list of the current running props, conf configurations along with a file path from which the configuration was made
Answer: C (LEAVE A REPLY)
Explanation
https://docs.splunk.com/Documentation/Splunk/8.0.1/Troubleshooting/Usebtooltotroubleshootconfigurations
"The btool command simulates the merging process using the on-disk conf files and creates a report showing the merged settings."
"The report does not necessarily represent what's loaded in memory. If a conf file change is made that requires a service restart, the btool report shows the change even though that change isn't active."

NEW QUESTION: 163
Which setting in indexes. conf allows data retention to be controlled by time?
A. maxDataRetentionTime
B. maxDaysToKeep
C. moveToFrozenAfter
D. frozenTimePeriodInSecs
Answer: C (LEAVE A REPLY)

NEW QUESTION: 164
Which of the following is valid distribute search group?
A)
```
[distributedSearch:Paris]
default = false
servers = server1, server2
```
B)
```
[searchGroup:Paris]
default = false
servers = server1:8089, server2:8089
```
C)
```
[searchGroup:Paris]
default = false
servers = server1:9997, server2:9997
```
D)
```
[distributedSearch:Paris]
default = false
servers = server1:8089, server2:8089
```
A. Option D
B. Option B
C. option A

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

NEW QUESTION: 165
During search time, which directory of configuration files has the highest precedence?
A. $SFLUNK_KOME/etc/system/local
B. $SPLUNK_KCME/etc/system/default
C. $SPLUNK_HCME/etc/apps/app1/local
D. $SPLUNK HCME/etc/users/admin/local
Answer: D (LEAVE A REPLY)
Adding further clarity and quoting same Splunk reference URL from @giubal"
"To keep configuration settings consistent across peer nodes, configuration files are managed from the cluster master, which pushes the files to the slave-app directories on the peer nodes.
Files in the slave-app directories have the highest precedence in a cluster peer's configuration. Here is the expanded precedence order for cluster peers:
1.Slave-app local directories -- highest priority
2. System local directory
3. App local directories
4. Slave-app default directories
5. App default directories
6. System default directory --lowest priority

NEW QUESTION: 166
What is the difference between the two wildcards ... and - for the monitor stanza in inputs, conf?
A. There is no difference, they are interchangable and match anything beyond directory boundaries.
B. ... matches anything in that specific directory path segment, whereas - recurses through subdirectories as well.
C. ... is not supported in monitor stanzas
D. * matches anything in that specific directory path segment, whereas ... recurses through subdirectories as well.
Answer: B (LEAVE A REPLY)

Valid SPLK-1003 Dumps shared by TrainingDump.com for Helping Passing SPLK-1003 Exam! TrainingDump.com now offer the **newest SPLK-1003 exam dumps**, the TrainingDump.com SPLK-1003 exam **questions have been updated** and **answers have been corrected** get the **newest** TrainingDump.com SPLK-1003 dumps with Test Engine here:
https://www.trainingdump.com/Splunk/SPLK-1003-practice-exam-dumps.html (**232** Q&As Dumps, **40%OFF** **Special Discount:** **Exam-Tests**)

NEW QUESTION: 167
When deploying apps, which attribute in the forwarder management interface determines the apps that clients install?
A. App Class
B. Client Class
C. Server Class
D. Forwarder Class
Answer: C (LEAVE A REPLY)

<https://docs.splunk.com/Documentation/Splunk/8.0.6/Updating/Deploymentserverarchitecture>
https://docs.splunk.com/Splexicon:Serverclass

NEW QUESTION: 168
Which of the following are required when defining an index in indexes. conf? (select all that apply)
A. homePath
B. thawedPath
C. frozenPath
D. coldPath
Answer: A,B,D (LEAVE A REPLY)

NEW QUESTION: 169
Consider a company with a Splunk distributed environment in production. The Compliance Department wants to start using Splunk; however, they want to ensure that no one can see their reports or any other knowledge objects. Which Splunk Component can be added to implement this policy for the new team?
A. Search head
B. Universal forwarder
C. Deployment server
D. Indexer
Answer: A (LEAVE A REPLY)

NEW QUESTION: 170
How does the Monitoring Console monitor forwarders?
A. With internal logs forwarded by forwarders.
B. With internal logs forwarder by deployment server.
C. By pulling internal logs from forwarders.
D. By using the forwarder monitoring add-on.
Answer: C (LEAVE A REPLY)

NEW QUESTION: 171
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: 172
Which of the following methods will connect a deployment client to a deployment server? (select all that apply)
A. Run $SPLUNK_ROME/bin/ splunk set deploy-poll : from the command line of the deployment client.
B. Create and edit a deploymentserver . conf file in SSPLVNE{ on the deployment server.

C. Create and edit a deploymentclient . conf file in SSPLTJNE(EOME/etc/ system/local on the deployment client.
D. Run $SPLUNK ROME/bin/spiunk set deploy-poi i : from the command line of the deployment server.
Answer: (SHOW ANSWER)
Explanation
The correct methods to connect a deployment client to a deployment server are A and C. You can either run the command splunk set deploy-poll <IP_address/hostname>:<management_port> from the command line of the deployment client1 or create and edit a deploymentclient.conf file in $SPLUNK_HOME/etc/system/local on the deployment client2. Both methods require you to specify the IP address, hostname, and management port of the deployment server that you want the client to connect to.

NEW QUESTION: 173
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/AcctID=\d{3}(\d{4})/AcctID=xxx\1/g
B. SEDCMD-1acct = s/AcctID=\d{3}(\d{4})/AcctID=\1xxx/g
C. SEDCMD-xxxAcct = s/AcctID=\d{3}(\d{4})/AcctID=xxx/g
D. SEDCMD-1acct = s/VendorID=\d{3}(\d{4})/VendorID=xxx/g
Answer: B (LEAVE A REPLY)

NEW QUESTION: 174
Which of the following enables compression for universal forwarders in outputs. conf ?
A)

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

B)

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

C)

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

D)

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

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

NEW QUESTION: 175

How is data handled by Splunk during the input phase of the data ingestion process?
A. Data is treated as streams.
B. Data is broken up into events.
C. Data is initially written to disk.
D. Data is measured by the license meter.
Answer: (SHOW ANSWER)
Explanation
https://docs.splunk.com/Documentation/Splunk/8.0.5/Deploy/Datapipeline
"In the input segment, Splunk software consumes data. It acquires the raw data stream from its source, breaks in into 64K blocks, and annotates each block with some metadata keys."

NEW QUESTION: 176
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: 177
A Universal Forwarder is collecting two separate sources of data (A,B). Source A is being routed through a Heavy Forwarder and then to an indexer. Source B is being routed directly to the indexer. Both sets of data require the masking of raw text strings before being written to disk. What does the administrator need to do to ensure that the masking takes place successfully?
A. Make sure that props . conf and transforms . conf are both present on the in-dexer and the search head.
B. For source A, make sure that props . conf is in place on the indexer; and for source B, make sure transforms . conf is present on the Heavy Forwarder.
C. Make sure that props . conf and transforms . conf are both present on the Universal Forwarder.
D. Place both props . conf and transforms . conf on the Heavy Forwarder for source A, and place both props . conf and transforms . conf on the indexer for source B.
Answer: D (LEAVE A REPLY)
Explanation
The correct answer is D. Place both props . conf and transforms . conf on the Heavy Forwarder for source A, and place both props . conf and transforms . conf on the indexer for source B.
According to the Splunk documentation1, to mask sensitive data from raw events, you need to use the SEDCMD attribute in the props.conf file and the REGEX attribute in the transforms.conf file. The SEDCMD attribute applies a sed expression to the raw data before indexing, while the REGEX attribute defines a regular expression to match the data to be masked.You need to place these files on the Splunk instance that parses the data, which is usually the indexer or the heavy forwarder2. The universal forwarder does not parse the data, so it does not need these files.
For source A, the data is routed through a heavy forwarder, which can parse the data before sending it to the indexer. Therefore, you need to place both props.conf and transforms.conf on the heavy forwarder for source A, so that the masking takes place before indexing.
For source B, the data is routed directly to the indexer, which parses and indexes the data. Therefore, you need to place both props.conf and transforms.conf on the indexer for source B, so that the masking takes place before indexing.
References:1:Redact data from events - Splunk Documentation2:Where do I configure my Splunk settings? - Splunk Documentation

NEW QUESTION: 178
What is the default value of LINE_BREAKER?
A. \r\n
B. ([\r\n]+)
C. \r+\n+
D. (\r\n+)
Answer: (SHOW ANSWER)
Reference:
Line breaking, which uses the LINE_BREAKER setting to split the incoming stream of data into separate lines. By default, the LINE_BREAKER value is any sequence of newlines and carriage returns. In regular expression format, this is represented as the following string: ([\r\n]+). You don't normally need to adjust this setting, but in cases where it's necessary, you must configure it in the props.conf configuration file on the forwarder that sends the data to Splunk Cloud Platform or a Splunk Enterprise indexer. The LINE_BREAKER setting expects a value in regular expression format.

NEW QUESTION: 179
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: (SHOW ANSWER)
Explanation
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: 180
All search-time field extractions should be specified on which Splunk component?
A. Deployment server
B. Universal forwarder
C. Indexer
D. Search head
Answer: D (LEAVE A REPLY)
Explanation
Search-time field extractions are the process of extracting fields from events after they are indexed.
Search-time field extractions are specified on the search head, which is the Splunk component that handles searching and reporting. Search-time field extractions are configured in props.conf and transforms.conf files, which are located in the etc/system/local directory on the search head. Therefore, option D is the correct answer. References: Splunk Enterprise Certified Admin | Splunk, [About fields - Splunk Documentation]

NEW QUESTION: 181
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.
Answer: D (LEAVE A REPLY)
Explanation/Reference: https://answers.splunk.com/answers/447096/how-to-remove-missing-forwarders-from-the- distribu.html

Valid SPLK-1003 Dumps shared by TrainingDump.com for Helping Passing SPLK-1003 Exam! TrainingDump.com now offer the **newest SPLK-1003 exam dumps**, the TrainingDump.com SPLK-1003 exam **questions have been updated** and **answers have been corrected** get the **newest** TrainingDump.com SPLK-1003 dumps with Test Engine here:
https://www.trainingdump.com/Splunk/SPLK-1003-practice-exam-dumps.html (**232** Q&As Dumps, **40%OFF** **Special Discount:** **Exam-Tests**)

NEW QUESTION: 182
When would the following command be used?

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

A. To verify' the integrity of a local index.
B. To verify the integrity of a SmartStore index.
C. To verify the integrity of a SmartStore bucket.
D. To verify the integrity of a local bucket.
Answer: D (LEAVE A REPLY)
Explanation
To verify the integrity of a local bucket. The command ./splunk check-integrity -bucketPath [bucket path]
[-verbose] is used to verify the integrity of a local bucket by comparing the hashes stored in the l1Hashes and l2Hash files with the actual data in the bucket1. This command can help detect any tampering or corruption of the data.

NEW QUESTION: 183
What are the values forhostandindexfor[stanza1]used by Splunk during index time, given the following configuration files?



A. host=server1
index=unixinfo
B. host=server1
index=searchinfo
C. host=searchsvr1
index=searchinfo
D. host=unixsvr1
index=unixinfo
Answer: A (LEAVE A REPLY)
Explanation
- etc/system/local/ has better precedence at index time - for identical settings in the same file, the last one overwrite others, see :https://community.splunk.com/t5/Getting-Data-In/What-is-the-precedence-for-identical-stanzas-within-a-single/

NEW QUESTION: 184
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
Answer: C (LEAVE A REPLY)
Explanation/Reference: https://docs.splunk.com/Documentation/Splunk/7.3.1/Admin/HowSplunklicensingworks

NEW QUESTION: 185
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: (SHOW ANSWER)
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

Valid SPLK-1003 Dumps shared by TrainingDump.com for Helping Passing SPLK-1003 Exam! TrainingDump.com now offer the **newest SPLK-1003 exam dumps**, the TrainingDump.com SPLK-1003 exam **questions have been updated** and **answers have been corrected** get the **newest** TrainingDump.com SPLK-1003 dumps with Test Engine here:
https://www.trainingdump.com/Splunk/SPLK-1003-practice-exam-dumps.html (**232** Q&As Dumps, **40%OFF** **Special Discount:** **Exam-Tests**)