Splunk.SPLK-1005.v2026-09-08.q47

Exam Code:	SPLK-1005
Exam Name:	Splunk Cloud Certified Admin
Certification Provider:	Splunk
Free Question Number:	47
Version:	v2026-09-08
# of views:	112
# of Questions views:	490
https://www.freecram.net/torrent/Splunk.SPLK-1005.v2026-09-08.q47.html	

NEW QUESTION: 1
Which of the following is the default bandwidth limit in the Splunk Universal Forwarder credentials package?
A. 0KBps
B. 256 KBps
C. 512 KBps
D. 1024 KBps
Answer: (SHOW ANSWER)
The default bandwidth limit in the Splunk Universal Forwarder is set to 256 KBps. This setting is in place to prevent the forwarder from overwhelming network resources, and it can be adjusted as necessary based on the deployment's specific needs.

NEW QUESTION: 2
Which statement best describes the primary purpose of sourcetypes during Splunk event processing operations?
A. Sourcetypes identify event formats and control parsing behavior during ingestion processing automatically.
B. Sourcetypes authenticate users and assign administrative permissions within distributed search infrastructures securely.
C. Sourcetypes replace indexes entirely when organizing searchable historical event storage repositories permanently.
D. Sourcetypes permanently determine retention policies and storage allocation for indexed enterprise datasets globally.
Answer: (SHOW ANSWER)

NEW QUESTION: 3
Which of the following tasks is not managed by the Splunk Cloud administrator?
A. Forwarding events to Splunk Cloud.
B. Upgrading the indexer's Splunk software.
C. Managing knowledge objects.
D. Creating users and roles.
Answer: (SHOW ANSWER)
In Splunk Cloud, several administrative tasks are managed by the Splunk Cloud administrator, but certain tasks related to the underlying infrastructure and core software management are handled by Splunk itself.

Upgrading the indexer's Splunk software is the correct answer. Upgrading Splunk software on indexers is a task that is managed by Splunk's operations team, not by the Splunk Cloud administrator. The Splunk Cloud administrator handles tasks like forwarding events, managing knowledge objects, and creating users and roles, but the underlying software upgrades and maintenance are managed by Splunk as part of the managed service.

NEW QUESTION: 4
Which of the following are default Splunk Cloud user roles?
A. must_delete, power, sc_admin
B. power, user, admin
C. apps, power, sc_admin
D. can delete, users, admin
Answer: (SHOW ANSWER)
Default Splunk Cloud roles include power, user, and admin, each with unique permissions suitable for common operational and administrative functions.

NEW QUESTION: 5
Which of the following app installation scenarios can be achieved without involving Splunk Support?
A. Deploy premium apps.
B. Install apps via the Request Install button.
C. Install apps via self-service.
D. Install apps that have not gone through the vetting process.
Answer: (SHOW ANSWER)
In Splunk Cloud, you can install apps via self-service, which allows you to install certain approved apps without involving Splunk Support. This self-service capability is provided for apps that have already been vetted and approved for use in the Splunk Cloud environment.

NEW QUESTION: 6
What does the followTail attribute do in inputs.conf?
A. Pauses a file monitor if the queue is full.
B. Only creates a tail checkpoint of the monitored file.
C. Ingests a file starting with new content and then reading older events.
D. Prevents pre-existing content in a file from being ingested.
Answer: (SHOW ANSWER)
The followTail attribute in inputs.conf controls how Splunk processes existing content in a monitored file.
When followTail = true is set, Splunk will ignore any pre-existing content in a file and only start monitoring from the end of the file, capturing new data as it is added. This is useful when you want to start monitoring a log file but do not want to index the historical data that might be present in the file.

NEW QUESTION: 7
Which configuration shown is used to enable a forwarder as a deployment client of the server
10.1.2.3?
A. [target-broker:deploymentServer] targetUri = 10.1.2.3:9997
B. [target-broker:deploymentserver] targetUri = 10.1.2.3:8089
C. [target-broker:deploymentserver] deploymentserver = 10.1.2.3:9997
D. [target-broker:deploymentserver] deploymentserver = 10.1.2.3:8089

Answer: (SHOW ANSWER)
For setting up a deployment client, the correct stanza syntax in inputs.conf includes specifying targetUri with the port 8089, which is the management port for Splunk instances, not the data port 9997.

NEW QUESTION: 8
What Splunk command will allow an administrator to view the runtime configuration instructions for a monitored file in Inputs. cont on the forwarders?
A. ./splunk _internal call /services/data/input.3/filemonitor
B. ./splunk show config inputs.conf
C. ./splunk _internal rest /services/data/inputs/monitor
D. ./splunk show config inputs
Answer: (SHOW ANSWER)
To view the runtime configuration instructions for a monitored file in inputs.conf on the forwarder, the correct command to use involves accessing the internal REST API that provides details on data inputs. ./splunk _internal rest /services/data/inputs/monitor is the correct answer. This command uses Splunk's internal REST endpoint to retrieve information about monitored files, including their runtime configurations as defined in inputs.conf.

NEW QUESTION: 9
Which Splunk configuration file primarily controls retention policies and indexed storage management settings globally?
A. indexes.conf manages storage paths and retention durations for indexed enterprise event repositories.
B. outputs.conf specifies destination forwarding groups and load balancing communication configurations centrally worldwide.
C. inputs.conf configures monitored files and onboarding settings for enterprise application data sources.
D. authorize.conf defines user permissions and inherited administrative capabilities across distributed organizations securely.
Answer: (SHOW ANSWER)
indexes.conf controls index creation, storage paths, retention durations, and archive settings.
Administrators configure data lifecycle management here to ensure searchable event repositories meet operational, compliance, and storage efficiency requirements effectively.

NEW QUESTION: 10
Which file primarily defines event parsing rules and metadata assignments during Splunk indexing operations?

A. props.conf controls event parsing behavior and metadata assignments during indexing workflows automatically.
B. transforms.conf configures index retention periods and storage allocation for archived event repositories globally.
C. outputs.conf authenticates distributed searches and synchronizes enterprise user role inheritance configurations continuously.
D. indexes.conf defines browser interface themes and session timeout settings across enterprise environments centrally.
Answer: (SHOW ANSWER)
props.conf defines event parsing behavior, including timestamp extraction, line breaking, and metadata assignments. It works closely with transforms.conf to ensure consistent event interpretation and accurate field extraction throughout Splunk ingestion workflows.

NEW QUESTION: 11
Windows Input types are collected in Splunk via a script which is configurable using the GUI.
What is this type of input called?
A. Batch
B. Scripted

C. Modular
D. Front-end
Answer: (SHOW ANSWER)
Windows inputs in Splunk, particularly those that involve more advanced data collection capabilities beyond simple file monitoring, can utilize scripts or custom inputs. These are typically referred to as Modular Inputs.
Modular Inputs are designed to be configurable via the Splunk Web UI and can collect data using custom or predefined scripts, handling more complex data collection tasks. This is the type of input that is used for collecting Windows-specific data such as Event Logs, Performance Monitoring, and other similar inputs.

NEW QUESTION: 12
Which of the following are valid settings for file and directory monitor inputs?
A. host, index, source_length, _TCP_Routing, host_segment
B. host, index, sourcetype, _TCP_Routing, host_regex, host_segment
C. host, index, directory, host_regex, host_segment
D. host, index, sourcetype, _UDP_Routing, host_regex, host_segment
Answer: (SHOW ANSWER)
In Splunk, when configuring file and directory monitor inputs, several settings are available that control how data is indexed and processed. These settings are defined in the inputs.conf file.
Among the given options:
host: Specifies the hostname associated with the data. It can be set to a static value, or dynamically assigned using settings like host_regex or host_segment.
index: Specifies the index where the data will be stored.
sourcetype: Defines the data type, which helps Splunk to correctly parse and process the data.
TCP_Routing: Used to route data to specific indexers in a distributed environment based on TCP routing rules.
host_regex: Allows you to extract the host from the path or filename using a regular expression.
host_segment: Identifies the segment of the directory structure (path) to use as the host.
Given the options:
Option B is correct because it includes host, index, sourcetype, TCP_Routing, host_regex, and host_segment. These are all valid settings for file and directory monitor inputs in Splunk.

NEW QUESTION: 13
Which of the following statements is true about data transformations using SEDCMD?
A. Can only be used to mask or truncate raw data.
B. Configured in props.conf and transform.conf.
C. Can be used to manipulate the sourcetype per event.
D. Operates on a REGEX pattern match of the source, sourcetype, or host of an event.
Answer: A (LEAVE A REPLY)
SEDCMD is a directive used within the props.conf file in Splunk to perform inline data transformations. Specifically, it uses sed-like syntax to modify data as it is being processed.
Option A: This is the correct answer because SEDCMD is typically used to mask sensitive data, such as obscuring personally identifiable information (PII) or truncating parts of data to ensure privacy and compliance with security policies. It is not used for more complex transformations such as changing the sourcetype per event.

NEW QUESTION: 14
A customer has worked with their LDAP administrator to configure an LDAP strategy in Splunk.
The configuration works, and user Mia can log into Splunk using her LDAP Account. After some time, the Splunk Cloud administrator needs to move Mia from the user role to the power role.
How should they accomplish this?

A. Ask the LDAP administrator to move Mia's account to an appropriately mapped LDAP group.
B. Have Mia log into Splunk, then update her own role in user settings.
C. Create a role named Power in Splunk, then map Mia's account to that role.
D. Use the Cloud Monitoring Console app as an administrator to map Mia's account to the power role.
Answer: A (LEAVE A REPLY)
In Splunk Cloud, role-based access controls are managed by mapping LDAP groups to Splunk roles. Therefore, any change in roles should be managed by the LDAP administrator, who can adjust Mia's group to an LDAP group mapped to the power role.

NEW QUESTION: 15
Where is the recommended place to deploy input apps that are not permitted on Splunk Cloud?
A. Universal Forwarder or Heavy Forwarder.
B. Heavy Forwarder only.
C. Universal Forwarder only.
D. Apps cannot be installed on on-prem instances.
Answer: (SHOW ANSWER)
For input apps that are not permitted on Splunk Cloud, the recommended place to deploy them is on a Universal Forwarder or Heavy Forwarder. These forwarders handle data collection and preprocessing before sending the data to Splunk Cloud. This setup allows organizations to leverage apps and configurations that are not supported directly in the cloud environment.

NEW QUESTION: 16
What two files are used in the data transformation process?
A. parsing.conf and transforms.conf
B. props.conf and transforms.conf
C. transforms.conf and fields.conf
D. transforms.conf and sourcetypes.conf
Answer: (SHOW ANSWER)
props.conf and transforms.conf define data parsing, transformations, and routing rules, making them essential for data transformations.

NEW QUESTION: 17
What is the recommended method to test the onboarding of a new data source before putting it in production?
A. Send test data to a test index.
B. Send data to the associated production index.
C. Replicate Splunk deployment in a test environment.
D. Send data to the chance index.
Answer: (SHOW ANSWER)

The recommended method to test the onboarding of a new data source before putting it into production is to send test data to a test index. This approach allows you to validate data parsing, field extractions, and indexing behavior without affecting the production environment or data.

NEW QUESTION: 18
Which file or folder below is not a required part of a deployment app?
A. app.conf (in default or local)
B. local.meta
C. metadata folder
D. props.conf
Answer: D (LEAVE A REPLY)
When creating a deployment app in Splunk, certain files and folders are considered essential to ensure proper configuration and operation:
app.conf (in default or local): This is required as it defines the app's metadata and behaviors.
local.meta: This file is important for defining access permissions for the app and is often included.
metadata folder: The metadata folder contains files like local.meta and default.meta and is typically required for defining permissions and other metadata-related settings.
props.conf: While props.conf is essential for many Splunk apps, it is not mandatory unless you need to define specific data parsing or transformation rules. props.conf is the correct answer because, although it is commonly used, it is not a mandatory part of every deployment app. An app may not need data parsing configurations, and thus, props.conf might not be present in some apps.

NEW QUESTION: 19
Which Splunk component primarily enables distributed searching across multiple indexers and storage repositories simultaneously?
A. Search Heads coordinate distributed searches and present consolidated results to enterprise users centrally.
B. Universal Forwarders permanently store indexed enterprise logs for historical compliance reporting operations globally.
C. Deployment Servers authenticate distributed searches and archive event repositories for disaster recovery continuously.
D. Monitoring Console parses incoming application logs before indexing and long-term searchable storage automatically.
Answer: (SHOW ANSWER)
Search Heads coordinate distributed search requests across multiple indexers and aggregate returned results for users. They provide centralized search experiences, dashboards, and reporting capabilities without permanently storing indexed enterprise event repositories locally.

NEW QUESTION: 20
What can be used in a Splunk Cloud environment to create new sourcetypes?
A. Data Preview
B. props. conf can be edited directly from the GUI
C. Splunk's CLI
D. Deployment Server
Answer: A (LEAVE A REPLY)
In a Splunk Cloud environment, the Data Preview feature is used to create and test new sourcetypes. This feature allows you to upload sample data, configure parsing settings, and define sourcetypes interactively without directly editing configuration files like props.conf or using the CLI.

NEW QUESTION: 21
What syntax is required in inputs.conf to ingest data from files or directories?
A. A monitor stanza, sourcetype, and Index is required to ingest data.
B. A monitor stanza, sourcetype, index, and host is required to ingest data.

C. A monitor stanza and sourcetype is required to ingest data.
D. Only the monitor stanza is required to ingest data.
Answer: (SHOW ANSWER)
In Splunk, to ingest data from files or directories, the basic configuration in inputs.conf requires at least the following elements:
monitor stanza: Specifies the file or directory to be monitored.
sourcetype: Identifies the format or type of the incoming data, which helps Splunk to correctly parse it.
index: Determines where the data will be stored within Splunk. The host attribute is optional, as Splunk can auto-assign a host value, but specifying it can be useful in certain scenarios.
However, it is not mandatory for data ingestion.

NEW QUESTION: 22
Which of the following takes place during the input phase?
A. Splunk annotates data with only 3 metadata keys: host, source, and sourcetype.
B. Splunk sets the character encoding of the data.
C. Splunk looks at the contents of the data to apply the correct source.
D. Splunk breaks data into individual lines.
Answer: B (LEAVE A REPLY)
During the input phase in Splunk, the system processes incoming data by first setting the character encoding of the data. This step ensures that the data is correctly interpreted by Splunk, allowing it to be parsed and processed properly later in the pipeline. Other options describe actions that occur during later phases, such as parsing and indexing.

NEW QUESTION: 23
In which of the following situations should Splunk Support be contacted?
A. When a custom search needs tuning due to not performing as expected.
B. When an app on Splunkbase indicates Request Install.
C. Before using the delete command.
D. When a new role that mirrors sc_admin is required.
Answer: (SHOW ANSWER)
In Splunk Cloud, when an app on Splunkbase indicates "Request Install," it means that the app is not available for direct self-service installation and requires intervention from Splunk Support.
This could be because the app needs to undergo an additional review for compatibility with the managed cloud environment or because it requires special installation procedures. In these cases, customers need to contact Splunk Support to request the installation of the app. Support will ensure that the app is properly vetted and compatible with Splunk Cloud before proceeding with the installation.

NEW QUESTION: 24
Which common issue most frequently prevents successful onboarding of enterprise event data into Splunk environments?
A. Incorrect sourcetype assignments cause parsing failures and inaccurate field extraction behaviors frequently.
B. Monitoring Console dashboards display infrastructure metrics using unsupported visualization formatting standards globally.
C. Search Head clustering disables forwarding communications toward distributed indexing infrastructures automatically everywhere.
D. Deployment Servers permanently archive duplicate event repositories across isolated storage environments continuously.
Answer: (SHOW ANSWER)
Incorrect sourcetype assignments commonly disrupt parsing operations, timestamp recognition, and field extraction accuracy. These problems reduce search quality and operational visibility, making sourcetype validation an essential troubleshooting step during onboarding activities.

NEW QUESTION: 25

Which of the following statements is true regarding sedcmd?
A. SEDCMD can be defined in either props.conf or transforms.conf.
B. SEDCMD does not work on Windows-based installations of Splunk.
C. SEDCMD uses the same syntax as Splunk's replace command.
D. SEDCMD provides search and replace functionality using regular expressions and substitutions.
Answer: (SHOW ANSWER)
SEDCMD in props.conf applies regular expressions to modify data as it is ingested. It is useful for transforming raw event data before indexing.

NEW QUESTION: 26
Which Splunk component primarily provides centralized operational visibility into distributed deployment health metrics continuously?
A. Monitoring Console displays infrastructure health dashboards and distributed performance statistics comprehensively.
B. Universal Forwarders generate indexed reports and visual dashboards for enterprise compliance auditing automatically.
C. Deployment Server permanently stores archived security events for long-term forensic investigations globally.
D. Search Heads enforce ingestion quotas and validate licensing compliance across clustered infrastructures continuously.
Answer: A (LEAVE A REPLY)
Monitoring Console provides centralized dashboards displaying indexing throughput, search performance, and infrastructure health metrics. Administrators use it to identify operational bottlenecks, troubleshoot distributed deployments, and monitor Splunk environment stability proactively.

NEW QUESTION: 27
What is the default port for sending data via HTTP Event Collector to Splunk Cloud?
A. 443
B. 8088
C. 9997
D. 8000
Answer: (SHOW ANSWER)
The default port for HTTP Event Collector (HEC) in Splunk Cloud is 8088, which is used for data ingestion via HEC.

NEW QUESTION: 28
Which of the following files is used for both search-time and index-time configuration?
A. props.conf
B. macros.conf
C. savesearch.conf
D. inputs.conf
Answer: (SHOW ANSWER)

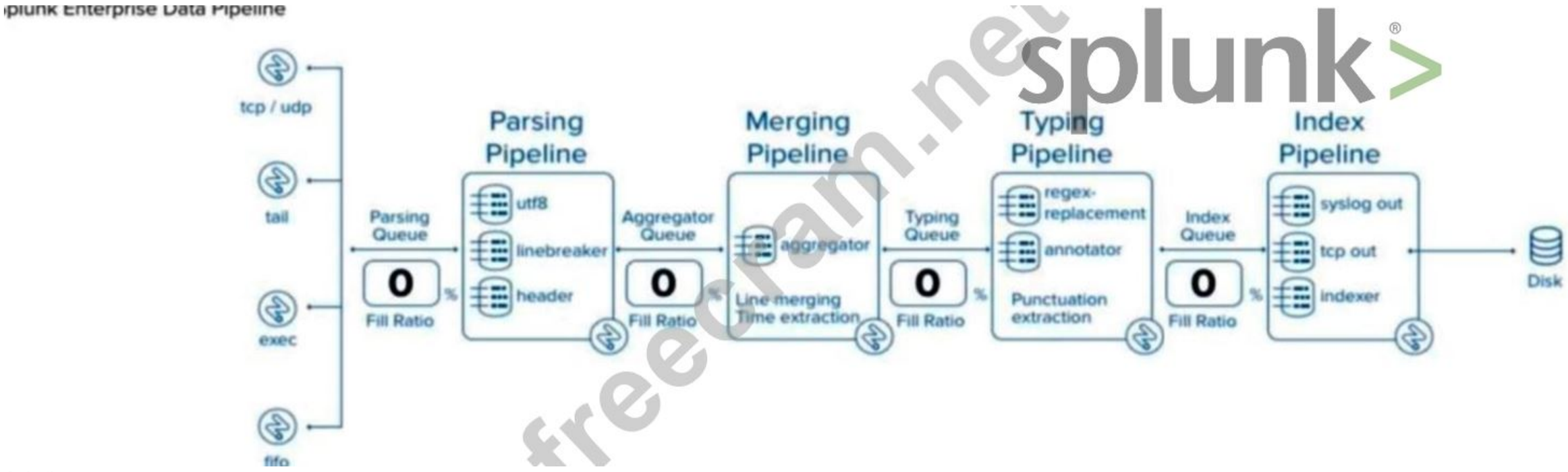
NEW QUESTION: 29
Which of the following stanzas would enable a TCP input on port 1025, allowing traffic from all IP addresses except 10.5.5.1?
A. [tcp://10.5.5.1:1025]
B. [tcp://1025]
acceptFrom = !10.5.5.1
C. [tcp://1025]

D. [tcp://1025]
acceptFrom = 10.5.5.1
Answer: (SHOW ANSWER)
In Splunk, to configure a TCP input on a specific port and restrict traffic from certain IP addresses, you can use the acceptFrom setting. The correct stanza that enables a TCP input on port 1025 and allows traffic from all IP addresses except 10.5.5.1 would look like this:
[tcp://1025]
acceptFrom = !10.5.5.1
Here, !10.5.5.1 denotes that traffic from this IP should be denied, while all other IP addresses are allowed.

NEW QUESTION: 30
Which of the following tasks is the responsibility of a Splunk Cloud administrator?
A. Configuring deployer
B. Configuring cluster master
C. Configuring indexers
D. Configuring indexes
Answer: (SHOW ANSWER)
In Splunk Cloud, configuring indexes is one of the primary responsibilities of a Splunk Cloud administrator. This task includes setting up new indexes, managing retention policies, and configuring index settings as required by the organization's data retention and compliance policies. Other tasks like configuring deployer, cluster master, or indexers are typically handled by Splunk Enterprise administrators, not Splunk Cloud administrators. Splunk Documentation

NEW QUESTION: 31
Files from multiple systems are being stored on a centralized log server. The files are organized into directories based on the original server they came from. Which of the following is a recommended approach for correctly setting the host values based on their origin?
A. Use the host segment, setting.
B. Set host = * in the monitor stanza.
C. The host value cannot be dynamically set.
D. Manually create a separate monitor stanza for each host, with the nose = value set.
Answer: (SHOW ANSWER)
The recommended approach for setting the host values based on their origin when files from multiple systems are stored on a centralized log server is to use the host_segment setting. This setting allows you to dynamically set the host value based on a specific segment of the file path, which can be particularly useful when organizing logs from different servers into directories.

NEW QUESTION: 32
At what point in the indexing pipeline set is SEDCMD applied to data?



A. In the aggregator queue
B. In the parsing queue
C. In the exec pipeline
D. In the typing pipeline
Answer: (SHOW ANSWER)
In Splunk, SEDCMD (Stream Editing Commands) is applied during the Typing Pipeline of the data indexing process.
The Typing Pipeline is responsible for various tasks, such as applying regular expressions for field extractions, replacements, and data transformation operations that occur after the initial parsing and aggregation steps.
Here's how the indexing process works in more detail:
Parsing Pipeline: In this stage, Splunk breaks incoming data into events, identifies timestamps, and assigns metadata.
Merging Pipeline: This stage is responsible for merging events and handling time-based operations.
Typing Pipeline: The Typing Pipeline is where SEDCMD operations occur. It applies regular expressions and replacements, which is essential for modifying raw data before indexing. This pipeline is also responsible for field extraction and other similar operations.
Index Pipeline: Finally, the processed data is indexed and stored, where it becomes available for searching.

NEW QUESTION: 33
The following Apache access log is being ingested into Splunk via a monitor input:

```
192.2.14.109 my.webserver.example - - 443 [09/Sep/2020:06:35:25 -0400] "GET / HTTP/1.1" "" 200 409 "-" "Mozilla/5.0
(Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/60.0.3112.113 Safari/537.36" 502 3110 1705
```

How does Splunk determine the time zone for this event?
A. The value of the TZ attribute in props. cont for the a :ces3_ccwbined sourcetype.
B. The value of the TZ attribute in props, conf for the my.webserver.example host.

C. The time zone of the Heavy/Intermediate Forwarder with the monitor input.
D. The time zone indicator in the raw event data.
Answer: (SHOW ANSWER)
In Splunk, when ingesting logs such as an Apache access log, the time zone for each event is typically determined by the time zone indicator present in the raw event data itself. In the log snippet you provided, the time zone is indicated by -0400, which specifies that the event's timestamp is 4 hours behind UTC (Coordinated Universal Time).
Splunk uses this information directly from the event to properly parse the timestamp and apply the correct time zone. This ensures that the event's time is accurately reflected regardless of the time zone in which the Splunk instance or forwarder is located. Splunk Cloud Reference: For further details, you can review Splunk documentation on timestamp recognition and time zone handling, especially in relation to log files and data ingestion configurations.

NEW QUESTION: 34
A Splunk Cloud administrator is looking to allow a new group of Splunk users in the marketing department to access the Splunk environment and view a dashboard with relevant data. These users need to access marketing data (stored in the marketing_data index), but shouldn't be able to access other data, such as events related to security or operations.
Which approach would be the best way to accomplish these requirements?
A. Create a new user with access to the marketing_data index assigned.
B. Create a new role that inherits the user role and remove the capability to search indexes other than marketing_data.
C. Create a new role that inherits the admin rote and assign access to the marketing_dat.a index.
D. Create a new role that does not inherit from any other role, turn on the same capabilities as the user role, and assign access to the marketing_data index.
Answer: (SHOW ANSWER)
The best approach to meet the requirements of the marketing department is to create a new role that inherits the user role but with restricted access to only the marketing_data index. This setup allows users to perform searches and view dashboards while ensuring they cannot access other indexes such as those containing security or operations data.

NEW QUESTION: 35
When is data deleted from a Splunk Cloud index?
A. When buckets roll to frozen, without a defined archive.
B. When data is deleted via the Splunk Cloud Admin GUI.
C. When TA_Delete is downloaded and enabled from SplunkBase.
D. When the daleteindex command is executed from the CLI.
Answer: (SHOW ANSWER)
In Splunk Cloud, data is deleted from an index when the buckets roll to the frozen stage and no archive is defined. When data in a bucket reaches the frozen stage, it is deleted unless a frozen- to- archival script is configured to move the data elsewhere. This process is part of the index lifecycle management in Splunk.

NEW QUESTION: 36
Which of the following methods is valid for creating index-time field extractions?
A. Use the UI to create a sourcetype, specify the field name and corresponding regular expression with capture statement.
B. Create a configuration app with the index-time props.conf and/or transfoms. conf, and upload the app via UI.
C. Use the CU app to define settings in fields.conf, and restart Splunk Cloud.
D. Use the rex command to extract the desired field, and then save as a calculated field.
Answer: (SHOW ANSWER)
The valid method for creating index-time field extractions is to create a configuration app that includes the necessary props.conf and/or transforms.conf configurations. This app can then be uploaded via the UI. Index-time field extractions must be defined in these configuration files to ensure that fields are extracted correctly during indexing.

NEW QUESTION: 37
When creating a new index, which of the following is true about archiving expired events?
A. Store expired events in private AWS-based storage.
B. Expired events cannot be archived.
C. Archive some expired events from an index and discard others.
D. Store expired events on-prem using your own storage systems.
Answer: D (LEAVE A REPLY)
In Splunk Cloud, expired events can be archived to customer-managed storage solutions, such as on-premises storage. This allows organizations to retain data beyond the standard retention period if needed.

NEW QUESTION: 38
When monitoring network inputs, there will be times when the forwarder is unable to send data to the indexers. Splunk uses a memory queue and a disk queue. Which setting is used for the disk queue?
A. queueSize
B. maxQeueSize
C. diskQiioiioiiizo
D. persistentQueueSize
Answer: (SHOW ANSWER)
When a forwarder is unable to send data to indexers, it queues the data in memory and optionally on disk. The setting used for the disk queue is persistentQueueSize. This configuration defines the size of the disk queue that stores data temporarily on the forwarder when it cannot immediately forward the data to an indexer.

NEW QUESTION: 39
When monitoring directories that contain mixed file types, which setting should be omitted from inputs, conf and instead be overridden in propo.conf?
A. sourcetype
B. host
C. source
D. index
Answer: (SHOW ANSWER)
When monitoring directories containing mixed file types, the sourcetype should typically be overridden in props.conf rather than defined in inputs.conf. This is because sourcetype is meant to classify the type of data being ingested, and when dealing with mixed file types, setting a single sourcetype in inputs.conf would not be effective for accurate data classification. Instead, you can use props.conf to define rules that apply different sourcetypes based on the file path, file name patterns, or other criteria. This allows for more granular and accurate assignment of sourcetypes, ensuring the data is properly parsed and indexed according to its type.

NEW QUESTION: 40
How is it possible to test a script from the Splunk perspective before using it within a scripted input?
A. splunk run <scriptname>
B. splunk script <scriptname>
C. ./$SPLUNK_HOME/etc/apps/<app>/bin/<scriptname>
D. splunk cmd <scriptname>
Answer: (SHOW ANSWER)
splunk cmd <scriptname> allows running scripts in Splunk's environment for testing purposes.
This ensures the script behaves as expected within Splunk's CLI context.

NEW QUESTION: 41
Which event ingestion method commonly transmits network and security logs using standardized logging protocols remotely?
A. Syslog forwarding securely transmits network device and security event logs toward Splunk infrastructures.
B. Deployment Server routing permanently archives firewall events before distributed indexing begins automatically worldwide.
C. Search Head clustering synchronizes network security policies across enterprise authentication infrastructures continuously globally.
D. License Manager parses syslog events and performs field extractions during distributed searching operations automatically.
Answer: (SHOW ANSWER)
Syslog forwarding is widely used for transmitting network, firewall, and security device logs toward Splunk environments. It provides standardized event communication and supports centralized operational monitoring and security analytics across enterprise infrastructures.

NEW QUESTION: 42
When using Splunk Universal Forwarders, which of the following is true?
A. No more than six Universal Forwarders may connect directly to Splunk Cloud.
B. Any number of Universal Forwarders may connect directly to Splunk Cloud.
C. Universal Forwarders must send data to an Intermediate Forwarder.
D. There must be one Intermediate Forwarder for every three Universal Forwarders.
Answer: (SHOW ANSWER)
Universal Forwarders can connect directly to Splunk Cloud, and there is no limit on the number of Universal Forwarders that may connect directly to it. This capability allows organizations to scale their data ingestion easily by deploying as many Universal Forwarders as needed without the requirement for intermediate forwarders unless additional data processing, filtering, or load balancing is required.

NEW QUESTION: 43
Configuration folders named default contain configuration files/settings specified in the Splunk product or default settings specified in apps. Which of the following is recommended to override these settings?
A. It does not matter whether setting overrides are placed in default or local folders. Both are equally acceptable since Splunk will merge all the files together into one runtime model after each restart.
B. Any settings to be overridden should be modified in-place wherever the setting was found originally. For example, if overriding a setting originally found in system/default, it should be overridden there to ensure that the desired value is used by Splunk.
C. Overrides should be placed in a folder named local, ideally within a custom Splunk app. This ensures the overrides are preserved upon product or app upgrade and will also be easier to maintain/support.
D. Try to store all configuration overrides in system/local folder to keep all configurations in one place.This ensures the modification has the highest precedence over all other configuration entries.
Answer: (SHOW ANSWER)
Placing configuration overrides in the local folder within a custom app allows for easy maintenance and ensures that these overrides are preserved during upgrades, as files in default are overwritten.

NEW QUESTION: 44
Due to internal security policies, a Splunk Cloud administrator cannot send data directly to Splunk Cloud from certain data sources. Additional parsing and API-based data sources also need to be sent to Splunk Cloud. What forwarder type should the Splunk Cloud administrator use to satisfy these requirements within their environment?
A. Syslog-ng server with a universal forwarder
B. Light forwarder as an intermediate forwarder
C. Heavy forwarder as an intermediate forwarder
D. Universal forwarder as an intermediate forwarder
Answer: (SHOW ANSWER)
A heavy forwarder is appropriate in this scenario because it can perform additional data parsing, filtering, and routing before forwarding data to Splunk Cloud. This is particularly useful for data that requires preprocessing or cannot be sent directly due to security policies.

NEW QUESTION: 45
Consider the following configurations:

```
$SPLUNK_HOME/etc/apps/unix/local/inputs.conf

    [monitor:///var/log/secure.log]
    sourcetype = access_combined
    index = security


$SPLUNK_HOME/etc/apps/search/local/inputs.conf

    [monitor:///var/log/secure.log]
    host = logsvr1
    sourcetype = linux_secure
```

What is the value of the sourcetype property for this stanza based on Splunk's configuration file precedence?
A. NULL, or unset, due to configuration conflict
B. access_corabined
C. linux aacurs
D. linux_secure, access_combined
Answer: (SHOW ANSWER)
When there are conflicting configurations in Splunk, the platform resolves them based on the configuration file precedence rules. These rules dictate which settings are applied based on the hierarchy of the configuration files.
In the provided configurations:
The first configuration in $SPLUNK_HOME/etc/apps/unix/local/inputs.conf sets the sourcetype to access_combined.
The second configuration in $SPLUNK_HOME/etc/apps/search/local/inputs.conf sets the sourcetype to linux_secure.

NEW QUESTION: 46
In which file can the SH0ULD_LINEMERCE setting be modified?
A. transforms.conf
B. inputs.conf
C. props.conf

D. outputs.conf
Answer: (SHOW ANSWER)
The SHOULD_LINEMERGE setting is used in Splunk to control whether or not multiple lines of an event should be combined into a single event. This setting is configured in the props.conf file, where Splunk handles data parsing and field extraction. Setting SHOULD_LINEMERGE = true merges lines together based on specific rules.

NEW QUESTION: 47
Which Splunk Cloud feature primarily provides centralized operational dashboards for distributed infrastructure monitoring activities?
A. Monitoring Console displays deployment health metrics and distributed search performance information centrally.
B. Deployment Server permanently stores archived security logs for forensic investigations across enterprises globally.
C. Universal Forwarders synchronize indexed events and retention settings across cloud storage infrastructures automatically.
D. Search Head clustering authenticates users and distributes application packages toward enterprise endpoints continuously.
Answer: (SHOW ANSWER)
Monitoring Console centralizes operational metrics including indexing throughput, resource utilization, and search latency. Administrators rely on its dashboards to proactively monitor distributed deployments and quickly identify infrastructure bottlenecks or performance degradation issues.

Valid SPLK-1005 Dumps shared by EduDump.com for Helping Passing SPLK-1005 Exam! EduDump.com now offer the **newest SPLK-1005 exam dumps**, the EduDump.com SPLK-1005 exam **questions have been updated** and **answers have been corrected** get the **newest** EduDump.com SPLK-1005 dumps with Test Engine here:
https://www.edudump.com/exams/Splunk/SPLK-1005/premium/ (**102** Q&As Dumps, **35%OFF** **Special Discount Code:** **freecram**)