[Feb 14, 2025 Get Free Updates Up to 365 days On Developing SPLK-1005 Braindumps [Q28-Q46

[Feb 14, 2025] Get Free Updates Up to 365 days On Developing SPLK-1005 Braindumps
Best Quality Splunk SPLK-1005 Exam Questions

To prepare for the SPLK-1005 exam, candidates can take advantage of Splunk's official training courses, such as the Splunk Cloud Administration course. Additionally, Splunk offers online resources, including documentation, blogs, and webinars, to help candidates prepare for the exam. Practicing with sample exams can also help candidates become familiar with the exam format and the types of questions asked.

NEW QUESTION 28

Which setting in inputs.conf can be used to specify the maximum size of a file that can be monitored by Splunk?
* max_file_size
* max_file_age
* max_file_count
* max_file_bytes

NEW QUESTION 29

What is the main advantage of self-service Splunk Cloud over managed Splunk Cloud in terms of cost and control?
* Self-service Splunk Cloud costs less to get started and maintain and allows your organization total control in setup and security configurations.
* Self-service Splunk Cloud costs more to get started and maintain but allows your organization total control in setup and security configurations.
* Self-service Splunk Cloud costs less to get started and maintain but requires your organization to rely on Splunk for setup and security configurations.
* Self-service Splunk Cloud costs more to get started and maintain and requires your organization to rely on Splunk for setup and security configurations.

NEW QUESTION 30

What is the name of the attribute that specifies the name of the stanza in the transforms.conf file that defines the data transformation in the props.conf file?
* REGEX
* FORMAT
* DEST_KEY
* TRANSFORMS

NEW QUESTION 31

Which of the following is true when using Intermediate Forwarders?
* Intermediate Forwarders may be a mix of Universal and Heavy Forwarders.
* All Intermediate Forwarders must be Heavy Forwarders.
* Intermediate Forwarders may be Universal Forwarders or Heavy Forwarders, but may not be mixed.
* All Intermediate Forwarders must be Universal Forwarders.
Intermediate Forwarders are special types of forwarders that sit between Universal Forwarders and indexers to perform additional processing tasks such as routing, filtering, or load balancing data before it reaches the indexers.

* B. All Intermediate Forwarders must be Heavy Forwardersis the correct answer. Heavy Forwarders are the only type of forwarder that can perform the necessary tasks required of an Intermediate Forwarder, such as parsing data, applying transformations, and routing based on specific rules.

Universal Forwarders are lightweight and cannot perform these complex tasks, thus cannot serve as Intermediate Forwarders.

Splunk Documentation References:

* Intermediate Forwarders

NEW QUESTION 32

Which of the following stanzas would enable a TCP input on port 1025, allowing traffic from all IP addresses except 10.5.5.1?
* `[tcp://10.5.5.1:1025]`
* `[tcp://1025]`
  `acceptFrom = !10.5.5.1`
* `[tcp://1025]`
* `[tcp://1025]`

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.

Therefore, Option B is correct.

Splunk Documentation Reference: Inputs.conf – acceptFrom

NEW QUESTION 33

Which command can be used to download and install the universal forwarder software on a Linux system?
* wget -O splunkforwarder-<version>-Linux-x86_64.tgz

‘https://www.splunk.com/bin/splunk/DownloadActivityServlet?architecture=x86_64&platform=linux&ve
* tar xvzf splunkforwarder-<version>-Linux-x86_64.tgz -C /opt
* /opt/splunkforwarder/bin/splunk start –accept-license
* All of the above

NEW QUESTION 34

In which file can the SH0ULD_LINEMERCE setting be modified?
* transforms.conf
* inputs.conf
* props.conf
* outputs.conf

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.

Splunk Documentation Reference: props.conf – SHOULD_LINEMERGE

NEW QUESTION 35

Which input type can be used to monitor Windows Registry Values for changes?
* WinRegMon
* WinRegistry
* WinRegValue

* WinRegChange

NEW QUESTION 36

Given the following set of files, which of the monitor stanzas below will result in Splunk monitoring all of the files ending with .log?

Files:

* /var/log/www1/secure.log

* /var/log/www1/access.log

* /var/log/www2/logs/secure.log

* /var/log/www2/access.log

* /var/log/www2/access.log.1
* [monitor:///var/log/*/*.log]
* [monitor:///var/log/…/*.log]
* [monitor:///var/log/*/*]
* [monitor:///var/log/…/*]

Explanation: The ellipsis (…) in [monitor:///var/log/…/*.log] allows Splunk to monitor files ending in .log in all nested directories under /var/log/. [Reference: Splunk Docs on monitor stanza syntax]

NEW QUESTION 37

Which type of forwarder can act as an intermediate forwarder to receive data from other forwarders and send it to the indexer?
* Universal forwarder
* Heavy forwarder
* Light forwarder
* Any type of forwarder

NEW QUESTION 38

Which configuration file parameter can be used to modify line termination settings interactively, using the Set Source Type page in Splunk Web?
* LINE_BREAKER
* SHOULD_LINEMERGE
* BREAK_ONLY_BEFORE
* TRUNCATE

NEW QUESTION 39

What is the name of the configuration file that governs data inputs such as forwarders and file system monitoring?
* inputs.conf
* props.conf
* transforms.conf
* outputs.conf

NEW QUESTION 40

What is the name of the configuration file where you can invoke data transformations by associating them with a host, source, or source type?
* limits.conf
* props.conf
* inputs.conf
* transforms.conf

NEW QUESTION 41

What is the name of the configuration file where you can specify the source type for a data input?
* limits.conf
* props.conf
* inputs.conf
* transforms.conf

NEW QUESTION 42

Which configuration file determines how a universal forwarder forwards data to the indexer?
* inputs.conf
* outputs.conf
* props.conf
* transforms.conf

NEW QUESTION 43

Which statement is true about monitor inputs?
* Monitor inputs are configured in the monitor, conf file.
* The ignoreOlderThan option allows files to be ignored based on the file modification time.
* ThecrSaltsetting is required.
* Monitor inputs can ignore a file’s existing content, indexing new data as it arrives, by configuring the tailProcessor option.

The statement about monitor inputs that is true is that the ignoreOlderThan option allows files to be ignored based on their file modification time. This setting helps prevent Splunk from indexing older data that is not relevant or needed.

Splunk Documentation Reference: Monitor files and directories

NEW QUESTION 44

Which option in Splunk Web can be used to create a new local TCP input?
* Settings > Data Inputs > TCP > New Local TCP
* Settings > Data Inputs > TCP > Add New
* Settings > Data Inputs > TCP > Create New
* Settings > Data Inputs > TCP > New Data Input

NEW QUESTION 45

Consider the following configurations:

What is the value of the sourcetypeproperty for this stanza based on Splunk’s configuration file precedence?
* NULL, or unset, due to configuration conflict
* access_corabined
* linux aacurs
* linux_secure, access_combined
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.

Configuration File Precedence:

* In Splunk, configurations in local directories take precedence over those in default.

* If two configurations are in local directories of different apps, the alphabetical order of the app names determines the precedence.

Since “search” comes after “unix” alphabetically, the configuration in $SPLUNK_HOME/etc/apps/search

/local/inputs.conf will take precedence.

Therefore, the value of the sourcetype property for this stanza islinux_secure.

Splunk Documentation References:

* Configuration File Precedence

* Resolving Conflicts in Splunk Configurations

This confirms that the correct answer isC. linux_secure.

NEW QUESTION 46

For the following data, what would be the correct attribute/value oair to use to successfully extract the correct timestamp from all the events?

* TIMK_FORMAT = %b %d %H:%M:%S %z
* DATETIME CONFIG= %Y-%m-%d %H:%M:%S %2
* TIME_FORMAT = %b %d %H:%M:%S
* DATETIKE CONFIG = Sb %d %H:%M:%S

The correct attribute/value pair to successfully extract the timestamp from the provided events is TIME_FORMAT = %b %d %H:%M:%S. This format corresponds to the structure of the timestamps in the provided data:

* %b represents the abbreviated month name (e.g., Sep).

* %d represents the day of the month.

* %H:%M:%S represents the time in hours, minutes, and seconds.

This format will correctly extract timestamps like “Sep 12 06:11:58”.

Splunk Documentation Reference: Configure Timestamp Recognition

The SPLK-1005 exam covers a range of topics related to Splunk Cloud administration, including installation, configuration, and maintenance of Splunk Cloud environments. Candidates will be tested on their ability to manage users and roles, configure data inputs and outputs, create and manage alerts and reports, and troubleshoot issues within a Splunk Cloud environment.

Splunk Exam Practice Test To Gain Brilliante Result:
https://www.testkingfree.com/Splunk/SPLK-1005-practice-exam-dumps.html]