SPLK-1003$^{Q\&As}$

Splunk Enterprise Certified Admin

Pass Splunk SPLK-1003 Exam with 100% Guarantee

Free Download Real Questions & Answers **PDF** and **VCE** file from:

https://www.geekcert.com/splk-1003.html

100% Passing Guarantee
100% Money Back Assurance

Following Questions and Answers are all new published by Splunk Official Exam Center

- **Instant Download** After Purchase
- **100% Money Back** Guarantee
- **365 Days** Free Update
- **800,000+** Satisfied Customers

QUESTION 1

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 defaultprops.confbelow, whichSPLUNK_HOME/etc/users/buttercup/myTA/local/props.confstanza 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
```

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

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

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

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

A. Option A

B. Option B

C. Option C

D. Option D

Correct Answer: B

https://docs.splunk.com/Documentation/Splunk/latest/Admin/Howtoeditaconfigurationfile#Clear%20a%20setting

QUESTION 2

What is the default value ofLINE_BREAKER?

A. \r\n

B. ([\r\n]+)

C. \r+\n+

D. (\r\n+)

Correct Answer: B

Reference:https://docs.splunk.com/Documentation/SplunkCloud/8.2.2105/Data/Configuree ventlinebreaking

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.

QUESTION 3

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

Correct Answer: B

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.

QUESTION 4

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

Correct Answer: D

When using a directory monitor input, specific source types can be selectively overridden using the props.conf file. According to the Splunk documentation, "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 file. 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 types. The transforms.conf file contains settings that modify or filter event dataduring indexing or search time. You can use these files to create rules that match specific patterns in the event data and assign different source types accordingly. 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 line.

QUESTION 5

How can native authentication be disabled in Splunk?

A. Remove the $SPLUNK_HOME/etc/passwd file

B. Create an empty $SPLUNK_HOME/etc/passwd file

C. Set SPLUNK_AUTHENTICATION=false in splunk-launch.conf

D. Set nativeAuthentication=false in authentication.conf

Correct Answer: B

Reference: https://docs.splunk.com/Documentation/Splunk/8.0.5/Security/Secureyouradminaccount