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.pass4itsure.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

SATISFACTION GUARANTEED
100%
SATISFACTION GUARANTEED

QUESTION 1

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. Indexer

B. Deployment server

C. Universal forwarder

D. Search head

Correct Answer: D

QUESTION 2

Which of the following are reasons to create separate indexes? (Choose all that apply.)

A. Different retention times.

B. Increase number of users.

C. Restrict user permissions.

D. File organization.

Correct Answer: AC

Reference:https://community.splunk.com/t5/Getting-Data-In/Why-does-Splunk-have- multiple-indexes/m-p/12063

Different retention times: You can set different retention policies for different indexes, depending on how long you want to keep the data. For example, you can have an index for security data that has a longer retention time than an index for performance data that has a shorter retention time.

Restrict user permissions: You can set different access permissions for different indexes, depending on who needs to see the data. For example, you can have an index for sensitive data that is only accessible by certain users or roles, and an index for public data that is accessible by everyone.

QUESTION 3

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.

Correct Answer: C

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]

QUESTION 4

Within props. conf, which stanzas are valid for data modification? (select all that apply)

A. Host

B. Server

C. Source

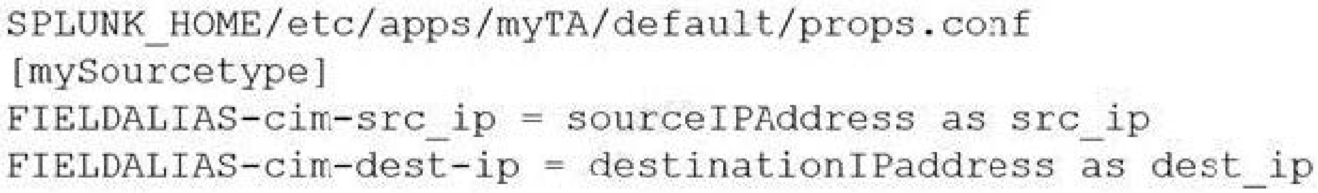
D. Sourcetype

Correct Answer: ACD

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

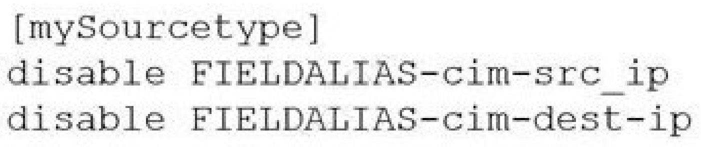
QUESTION 5

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?



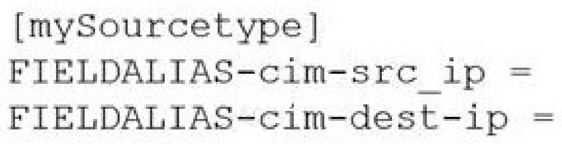
```
SPLUNK_HOME/etc/apps/myTA/default/props.conf
[mySourcetype]
FIELDALIAS-cim-src_ip = sourceIPAddress as src_ip
FIELDALIAS-cim-dest-ip = destinationIPaddress as dest_ip
```

A.



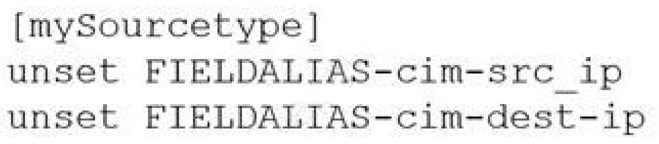
```
[mySourcetype]
disable FIELDALIAS-cim-src_ip
disable FIELDALIAS-cim-dest-ip
```

B.



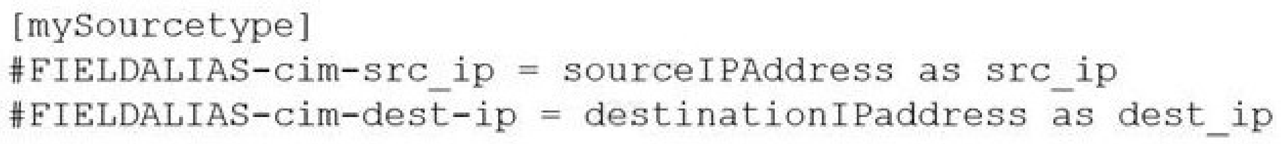
```
[mySourcetype]
FIELDALIAS-cim-src_ip =
FIELDALIAS-cim-dest-ip =
```

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

SPLK-1003 PDF Dumps   SPLK-1003 Study Guide   SPLK-1003 Exam Questions