

# Free Questions for SPLK-1003 by vceexamstest

Shared by Sandoval on 06-06-2022

For More Free Questions and Preparation Resources

**Check the Links on Last Page** 

<b>Question Type:</b> Multiple	Choice	oice
--------------------------------	--------	------

Which data pipeline phase is the last opportunity for defining event boundaries?

### **Options:**

- A- Input phase
- **B-** Indexing phase
- **C-** Parsing phase
- **D-** Search phase

#### **Answer:**

С

### **Explanation:**

Reference https://docs.splunk.com/Documentation/Splunk/8.2.3/Admin/Configurationparametersandthedatapipeline

**Question Type:** MultipleChoice

Which of the following Splunk components require a separate installation package?

### **Options:**

- A- Deployment server
- **B-** License master
- **C-** Universal forwarder
- **D-** Heavy forwarder

#### **Answer:**

С

# **Question 3**

**Question Type:** MultipleChoice

Which forward	der is recommen	ded by Splunk to	use in a production	environment?

#### **Options:**

- A- Heavy forwarder
- **B-** SSL forwarder
- C- Lightweight forwarder
- **D-** Universal forwarder

#### **Answer:**

D

### **Question 4**

**Question Type:** MultipleChoice

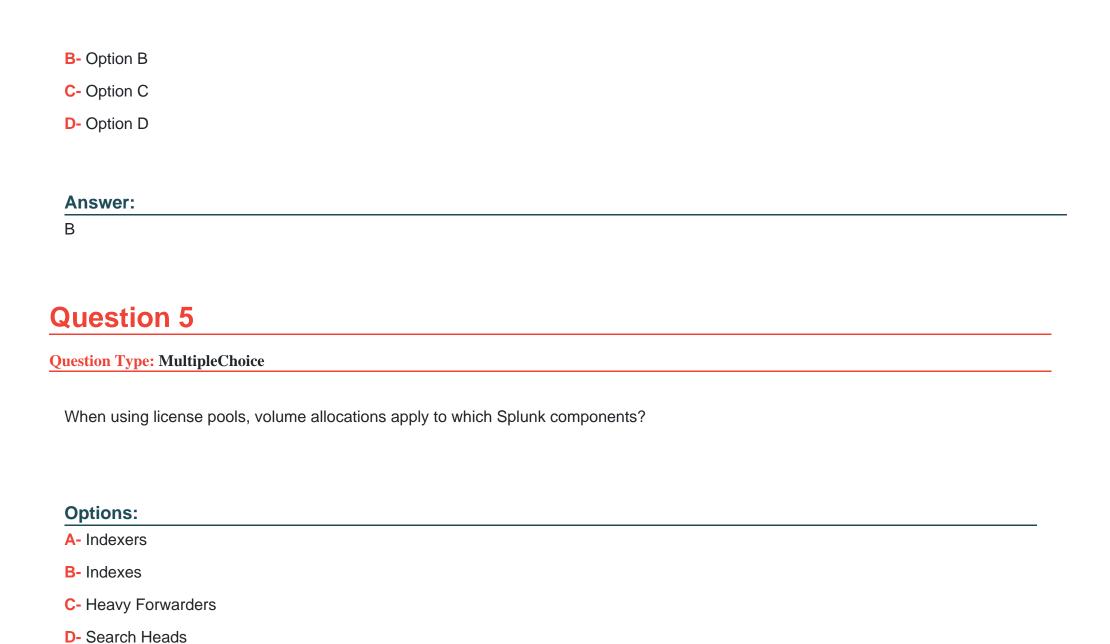
An add-on has configured field aliases for source IP address and destination IP address fields. A specific user prefers not to have those fields present in their user context. Based on the default props.conf below, which

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
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
```

#### **Options:**

A- Option A



Answer:
A
Question 6
Question Type: MultipleChoice
When using a directory monitor input, specific source type can be selectively overridden using which configuration file?
Options:
A- props.conf
B- sourcetypes.conf
C- transforms.conf
D- outputs.conf
Answer:

Α

#### **Question Type:** MultipleChoice

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?

#### **Options:**

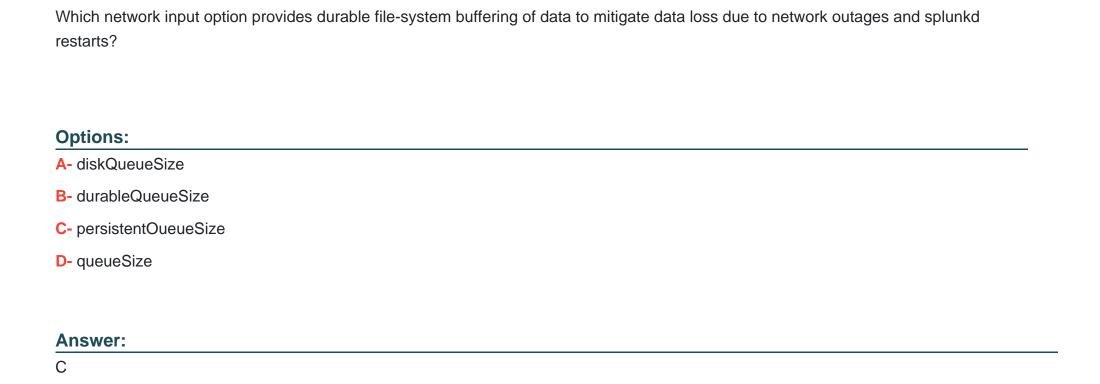
- A- Restart Splunk on the deployment server.
- B- Enable the deployment client in Splunk Web under Forwarder Management.
- C- Restart Splunk on the deployment client.
- D- Wait for up to the time set in the phoneHomeIntervalInSecs setting.

#### **Answer:**

Α

# **Question 8**

**Question Type:** MultipleChoice



**Question Type:** MultipleChoice

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

Options:
A- Different retention times.
B- Increase number of users.
C- Restrict user permissions.
D- File organization.
Answer:
A, D
Question 10
Question Type: MultipleChoice
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?

Options:
A- 21MB

- **B-** 28MB
- **C-** 14MB
- **D-** 7MB

### **Answer:**

Α

### To Get Premium Files for SPLK-1003 Visit

https://www.p2pexams.com/products/splk-1003

### **For More Free Questions Visit**

https://www.p2pexams.com/splunk/pdf/splk-1003

