Splunk SPLK-3001 Practice Questions

Shared by Maxwell on 18-08-2026

For More Free Questions and Preparation Resources

Check the Links on Last Page

Question 1

Question Type: MultipleChoice

Which tool Is used to update indexers In E5?

Options:

A- Index Updater
B- Distributed Configuration Management
C- indexes.conf
D- Splunk_TA_ForIndexeres. spl

Answer:

B

Question 2

Question Type: MultipleChoice

Which of the following is part of tuning correlation searches for a new ES installation?

Options:

A- Configuring correlation notable event index.
B- Configuring correlation permissions.
C- Configuring correlation adaptive responses.
D- Configuring correlation result storage.

Answer:

A

Question 3

Question Type: MultipleChoice

When ES content is exported, an app with a .spl extension is automatically created. What is the

best practice when exporting and importing updates to ES content?

Options:

A- Use new app names each time content is exported.
B- Do not use the .spl extension when naming an export.
C- Always include existing and new content for each export.
D- Either use new app names or always include both existing and new content.

Answer:

D

Explanation:

Either use new app names each time (which could be difficult to manage) or make sure you always include all content (old and new) each time you export.

Question 4

Question Type: MultipleChoice

Which column in the Asset or Identity list is combined with event security to make a notable event's urgency?

Options:

A- VIP
B- Priority
C- Importance
D- Criticality

Answer:

B

Question 5

Question Type: MultipleChoice

Which of the following features can the Add-on Builder configure in a new add-on?

Options:

A- Expire data.
B- Normalize data.
C- Summarize data.
D- Translate data.

Answer:

B

Question 6

Question Type: MultipleChoice

What kind of value is in the red box in this picture?

Additional Fields	Value
HTTP Method	GET
Source	10.98.27.195 500
Source Expected	false
Source PCI Domain	untrust
Source Requires Antivirus	false
Source Should Time Synchronize	false
Source Should Update	false
Tag	modaction_result

Options:

A- A risk score.
B- A source ranking.
C- An event priority.
D- An IP address rating.

Answer:

A

Question 7

Question Type: MultipleChoice

What are the steps to add a new column to the Notable Event table in the Incident Review dashboard?

Options:

A- Configure -> Incident Management -> Notable Event Statuses
B- Configure -> Content Management -> Type: Correlation Search
C- Configure -> Incident Management -> Incident Review Settings -> Event Management
D- Configure -> Incident Management -> Incident Review Settings -> Table Attributes

Answer:

D

Question 8

Question Type: MultipleChoice

Which option best is a key feature of a glass table?

Options:

A- Rigidity.
B- Customization.
C- Interactive investigations.
D- Strong data for later retrieval.

Answer:

B