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.passapply.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

When deploying apps, which attribute in the forwarder management interface determines the apps that clients install?

A. App Class

B. Client Class

C. Server Class

D. Forwarder Class

Correct Answer: C

https://docs.splunk.com/Splexicon:Serverclass

QUESTION 2

For single line event sourcetypes. it is most efficient to set SHOULD_linemerge to what value?

A. True

B. False

C.

D. Newline Character

Correct Answer: B

https://docs.splunk.com/Documentation/Splunk/latest/Data/Configureeventlinebreaking Attribute : SHOULD_LINEMERGE = [true|false]

Description : When set to true, the Splunk platform combines several input lines into a single event, with configuration based on the settings described in the next section.

QUESTION 3

Which of the methods listed below supports muti-factor authentication?

A. Lightweight Directory Access Protocol (LDAP)

B. Security Assertion Markup Language (SAML)

C. Single Sign-on (SSO)

D. OpenID

Correct Answer: B

SAML is an open standard for exchanging authentication and authorization data between parties, especially between an

identity provider and a service provider1. SAML supports multi-factor authentication by allowing the identity provider to require the user to present two or more factors of evidence to prove their identity2. For example, the user may need to enter a password and a one-time code sent to their phone, or scan their fingerprint and face.

QUESTION 4

Which of the following are required when defining an index in indexes. conf? (select all that apply)

A. coldPath

B. homePath

C. frozenPath

D. thawedPath

Correct Answer: ABD

homePath = $SPLUNK_DB/hatchdb/db coldPath = $SPLUNK_DB/hatchdb/colddb thawedPath = $SPLUNK_DB/hatchdb/thaweddb

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