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

What are the required stanza attributes when configuring the transforms. conf to manipulate or remove events?

A. REGEX, DEST. FORMAT

B. REGEX. SRC_KEY, FORMAT

C. REGEX, DEST_KEY, FORMAT

D. REGEX, DEST_KEY FORMATTING

Correct Answer: C

REGEX =

*

Enter a regular expression to operate on your data. FORMAT =

*

NOTE: This option is valid for both index-time and search-time field extraction. Index-time field extraction configuration require the FORMAT settings. The FORMAT settings is optional for search-time field extraction configurations.

*

This setting specifies the format of the event, including any field names or values you want to add. DEST_KEY =

*

NOTE: This setting is only valid for index-time field extractions.

*

Specifies where SPLUNK software stores the expanded FORMAT results in accordance with the REGEX match.

QUESTION 2

How would you configure your distsearch conf to allow you to run the search below? sourcetype=access_combined status=200 action=purchase splunk_setver_group=HOUSTON A)

```
[distributedSearch:NYC]
default = false
servers = nyc1:8089, nyc2:8089

[distributedSearch:HOUSTON]
default = false
servers = houston1:8089, houston2:8089
```

B)

```
[distributedSearch]
servers = nyc1, nyc2, houston1, houston2

[distributedSearch:NYC]
default = false
servers = nyc1, nyc2

[distributedSearch:HOUSTON]
default = false
servers = houston1, houston2
```

C)

```
[distributedSearch]
servers = nyc1:8089, nyc2:8089, houston1:8089, houston2:8089

[distributedSearch:NYC]
default = false
servers = nyc1:8089, nyc2:8089

[distributedSearch:HOUSTON]
default = false
servers = houston1:8089, houston2:8089
```

D)

```
[distributedSearch]
servers = nyc1:8089; nyc2:8089; houston1:8089; houston2:8089

[distributedSearch:NYC]
default = false
servers = nyc1:8089; nyc2:8089

[distributedSearch:HOUSTON]
default = false
servers = houston1:8089; houston2:8089
```

A. option A

B. Option B

C. Option C

D. Option D

Correct Answer: C

https://docs.splunk.com/Documentation/Splunk/8.0.3/DistSearch/Distributedsearchgroups

QUESTION 3

Which setting in indexes. conf allows data retention to be controlled by time?

A. maxDaysToKeep

B. moveToFrozenAfter

C. maxDataRetentionTime

D. frozenTimePeriodlnSecs

Correct Answer: D

https://docs.splunk.com/Documentation/Splunk/latest/Indexer/Setaretirementandarchivingpolicy

QUESTION 4

Which of the following must be done to define user permissions when integrating Splunk with LDAP?

A. Map Users

B. Map Groups

C. Map LDAP Inheritance

D. Map LDAP to Active Directory

Correct Answer: B

"You can map either users or groups, but not both. If you are using groups, all users must be members of an appropriate group. Groups inherit capabilities form the highest level role they\\'re a member of." "If your LDAP environment does not have group entries, you can treat each user as its own group."

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

QUESTION 5

What is the correct order of steps in Duo Multifactor Authentication?

A. 1 Request Login

2. Connect to SAML server

3 Duo MFA

4 Create User session

5 Authentication Granted 6. Log into Splunk

B. 1. Request Login 2 Duo MFA

3. Authentication Granted 4 Connect to SAML server

5.

Log into Splunk

6.

Create User session

C. 1 Request Login 2 Check authentication / group mapping 3 Authentication Granted

4.

Duo MFA

5.

Create User session

6.

Log into Splunk

D. 1 Request Login 2 Duo MFA

3. Check authentication / group mapping

4 Create User session

5. Authentication Granted

6 Log into Splunk

Correct Answer: C

Using the provided DUO/Splunk reference URL https://duo.com/docs/splunk

Scroll down to the Network Diagram section and note the following 6 similar steps: 1 - SPlunk connection initiated 2 - Primary authentication 3 - Splunk connection established to Duo Security over TCP port 443 4 - Secondary authentication via Duo Security\\'s service 5 - Splunk receives authentication response 6 - Splunk session logged in.