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.geekcert.com/splk-1003.html

100% Passing Guarantee
100% Money Back Assurance

Following Questions and Answers are all new published by Splunk Official Exam Center

QUESTION 1

Which authentication methods are natively supported within Splunk Enterprise? (select all that apply)

A. LDAP

B. SAML

C. RADIUS

D. Duo Multifactor Authentication

Correct Answer: ABC

Splunk authentication: Provides Admin, Power and User by default, and you can define your own roles using a list of capabilities. If you have an Enterprise license, Splunk authentication is enabled by default. See Set up user authentication with Splunk\\'s built-in system for more information. LDAP: Splunk Enterprise supports authentication with its internal authentication services or your existing LDAP server. See Set up user authentication with LDAP for more information. Scripted authentication API: Use scripted authentication to integrate Splunk authentication with an external authentication system, such as RADIUS or PAM. See Set up user authentication with external systems for more information. Note: Authentication, including native authentication, LDAP, and scripted authentication, is not available in Splunk Free.

QUESTION 2

Which configuration files are used to transform raw data ingested by Splunk? (Choose all that apply.)

A. props.conf

B. inputs.conf

C. rawdata.conf

D. transforms.conf

Correct Answer: AD

Reference: https://docs.splunk.com/Documentation/Splunk/8.0.5/Data/Configuretimestamprecognition

QUESTION 3

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 4

This file has been manually created on a universal forwarder

```
/opt/splunkforwarder/etc/apps/my_TA/local/inputs.conf

[monitor:///var/log/messages]
sourcetype=syslog
index=syslog
```

A new Splunk admin comes in and connects the universal forwarders to a deployment server and deploys the same app with a new

inputs.conf file:

```
/opt/splunk/etc/deployment-apps/my_TA/local/inputs.conf

[monitor:///var/log/maillog]
sourcetype=maillog
index=syslog
```

Which file is now monitored?

A. /var/log/messages

B. /var/log/maillog

C. /var/log/maillog and /var/log/messages

D. none of the above

Correct Answer: B

QUESTION 5

What is the difference between the two wildcards ... and * for the monitor stanza in inputs, conf?

A. ... is not supported in monitor stanzas

B. There is no difference, they are interchangable and match anything beyond directory boundaries.

C. * matches anything in that specific directory path segment, whereas ... recurses through subdirectories as well.

D. ... matches anything in that specific directory path segment, whereas - recurses through subdirectories as well.

Correct Answer: C

https://docs.splunk.com/Documentation/Splunk/7.3.0/Data/Specifyinputpathswithwildcards

The ellipsis wildcard searches recursively through directories and any number of levels of subdirectories to find matches. If you specify a folder separator (for example, //var/log/.../file), it does not match the first folder level, only subfolders.

* The asterisk wildcard matches anything in that specific folder path segment. Unlike ..., * does not recurse through subfolders.