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.pass2lead.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

How can native authentication be disabled in Splunk?

A. Remove the $SPLUNK_HOME/etc/passwd file

B. Create an empty $SPLUNK_HOME/etc/passwd file

C. Set SPLUNK_AUTHENTICATION=false in splunk-launch.conf

D. Set nativeAuthentication=false in authentication.conf

Correct Answer: B

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

QUESTION 2

Which feature of Splunk\\'s role configuration can be used to aggregate multiple roles intended for groups of users?

A. Linked roles

B. Grantable roles

C. Role federation

D. Role inheritance

Correct Answer: D

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

QUESTION 3

When running the command shown below, what is the default path in which deployment server.conf is created? splunk set deploy-poll deployServer:port

A. SFLUNK_HOME/etc/deployment

B. SPLUNK_HOME/etc/system/local

C. SPLUNK_HOME/etc/system/default

D. SPLUNK_KOME/etc/apps/deployment

Correct Answer: B

https://docs.splunk.com/Documentation/Splunk/8.1.1/Updating/Definedeploymentclasses#

Ways_to_define_server_classes "When you use forwarder management to create a new server class, it saves the server class definition in a copy of serverclass.conf under $SPLUNK_HOME/etc/system/local. If, instead of using forwarder

management, you decide to directly edit serverclass.conf, it is recommended that you create the serverclass.conf file in that same directory, $SPLUNK_HOME/etc/system/local."

QUESTION 4

Which of the following are supported options when configuring optional network inputs?

A. Metadata override, sender filtering options, network input queues (quantum queues)

B. Metadata override, sender filtering options, network input queues (memory/persistent queues)

C. Filename override, sender filtering options, network output queues (memory/persistent queues)

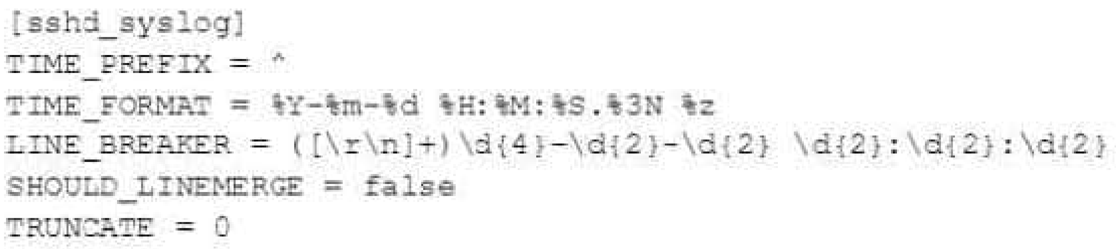
D. Metadata override, receiver filtering options, network input queues (memory/persistent queues)

Correct Answer: B

https://docs.splunk.com/Documentation/Splunk/latest/Data/Monitornetworkports

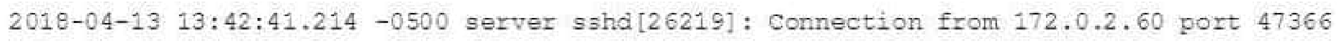
QUESTION 5

In this source definition the MAX_TIMESTAMP_LOOKHEAD is missing. Which value would fit best?



```
[sshd_syslog]
TIME_PREFIX = ^
TIME_FORMAT = %Y-%m-%d %H:%M:%S.%3N %z
LINE_BREAKER = ([\r\n]+)\d{4}-\d{2}-\d{2} \d{2}:\d{2}:\d{2}
SHOULD_LINEMERGE = false
TRUNCATE = 0
```

Event example:



```
2018-04-13 13:42:41.214 -0500 server sshd[26219]: Connection from 172.0.2.60 port 47366
```

A. MAX_TIMESTAMP_L0CKAHEAD = 5

B. MAX_TIMESTAMP_LOOKAHEAD - 10

C. MAX_TIMESTAMF_LOOKHEAD = 20

D. MAX TIMESTAMP LOOKAHEAD - 30

Correct Answer: D

https://docs.splunk.com/Documentation/Splunk/6.2.0/Data/Configuretimestamprecognition

"Specify how far (how many characters) into an event Splunk software should look for a timestamp." since TIME_PREFIX = ^ and timestamp is from 0-29 position, so D=30 will pick up the WHOLE timestamp correctly.

Latest SPLK-1003 Dumps SPLK-1003 PDF Dumps SPLK-1003 Braindumps