SPLK-1003$^{\text{Q\&As}}$

Splunk Enterprise Certified Admin

Pass Splunk SPLK-1003 Exam with 100% Guarantee

Free Download Real Questions & Answers **PDF** and **VCE** file from:

https://www.pass4itsure.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 Splunk forwarder type allows parsing of data before forwarding to an indexer?

A. Universal forwarder

B. Parsing forwarder

C. Heavy forwarder

D. Advanced forwarder

Correct Answer: C

QUESTION 2

How often does Splunk recheck the LDAP server?

A. Every 5 minutes

B. Each time a user logs in

C. Each time Splunk is restarted

D. Varies based on LDAP_refresh setting.

Correct Answer: B

https://docs.splunk.com/Documentation/Splunk/8.0.6/Security/ManageSplunkuserroleswith LDAP

QUESTION 3

What is the command to reset the fishbucket for one source?

A. rm -r ~/splunkforwarder/var/lib/splunk/fishbucket

B. splunk clean eventdata -index _thefishbucket

C. splunk cmd btprobe -d SPLUNK_HOME/var/lib/splunk/fishbucket/splunk_private_db -- file --reset

D. splunk btool fishbucket reset

Correct Answer: C

Reference:https://community.splunk.com/t5/Getting-Data-In/How-can-I-trigger-the-re- indexing-of-a-single-file/m-p/108568

The fishbucket is a directory that stores information about the files that have been monitored and indexed by Splunk. The fishbucket helps Splunk avoid indexing duplicate data by keeping track of file signatures and offsets. To reset the fishbucket for one source, the command splunk cmd btprobe can be used with the -reset option and the name of the source file. Therefore, option C is the correct answer. References: Splunk Enterprise Certified Admin | Splunk, [Use btprobe to troubleshoot file monitoring - Splunk Documentation]

QUESTION 4

The Splunk administrator wants to ensure data is distributed evenly amongst the indexers.

To do this, he runs the following search over the last 24 hours:

index=*

What field can the administrator check to see the data distribution?

A. host

B. index

C. linecount

D. splunk_server

Correct Answer: D

https://docs.splunk.com/Documentation/Splunk/8.2.2/Knowledge/Usedefaultfields splunk_server The splunk server field contains the name of the Splunk server containing the event. Useful in a distributed Splunk environment. Example: Restrict a search to the main index on a server named remote. splunk_server=remote index=main 404

QUESTION 5

When using a directory monitor input, specific source type can be selectively overridden using which configuration file?

A. props.conf

B. sourcetypes.conf

C. transforms.conf

D. outputs.conf

Correct Answer: A

Reference:https://docs.splunk.com/Documentation/SplunkCloud/latest/Data/Bypassautoma ticsourcetypeassignment

When using a directory monitor input, specific source types can be selectively overridden using props.conf. The props.conf file contains settings for parsing and indexing data, as well as search-time field extractions. The props.conf file can be used to assign or change source types for specific inputs using the sourcetype attribute. Therefore, option A is the correct answer. References: Splunk Enterprise Certified Admin | Splunk, [Configure directory monitor inputs - Splunk Documentation]

QUESTION 6

Which of the following methods will connect a deployment client to a deployment server? (select all that apply)

A. Run $SPLUNK_ROME/bin/ splunk set deploy-poll : from the command line of the deployment client.

B. Create and edit a deploymentserver . conf file in SSPLVNE{ on the deployment server.

C. Create and edit a deploymentclient . conf file in SSPLTJNE(EOME/etc/ system/local on the deployment client.

D. Run $SPLUNK ROME/bin/spiunk set deploy-poi i : from the command line of the deployment server.

Correct Answer: AC

The correct methods to connect a deployment client to a deployment server are A and C. You can either run the command splunk set deploy-poll : from the command line of the deployment client1 or create and edit a deploymentclient.conf file in $SPLUNK_HOME/etc/system/local on the deployment client2. Both methods require you to specify the IP address, hostname, and management port of the deployment server that you want the client to connect to.

QUESTION 7

What happens when the same username exists in Splunk as well as through LDAP?

A. Splunk user is automatically deleted from authentication.conf.

B. LDAP settings take precedence.

C. Splunk settings take precedence.

D. LDAP user is automatically deleted from authentication.conf

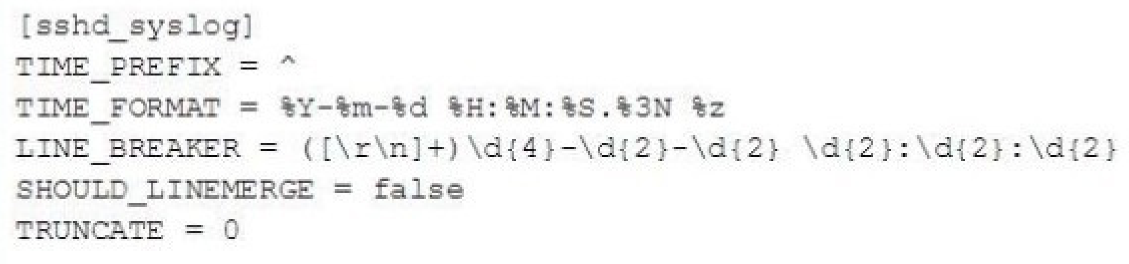
Correct Answer: C

Reference:https://docs.splunk.com/Documentation/SplunkCloud/8.2.2105/Security/SetupuserauthenticationwithLDAP

Splunk platform attempts native authentication first. If authentication fails outside of a local account that doesn\\'t exist, there is no attempt to use LDAP to log in. This is adapted from precedence of Splunk authentication schema.

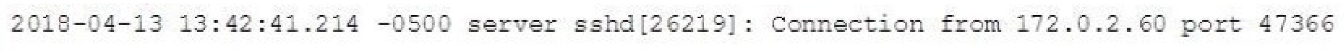
QUESTION 8

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 029 position, so D=30 will pick up the WHOLE timestamp correctly.

QUESTION 9

In case of a conflict between a whitelist and a blacklist input setting, which one is used?

A. Blacklist

B. Whitelist

C. They cancel each other out.

D. Whichever is entered into the configuration first.

Correct Answer: A

https://docs.splunk.com/Documentation/Splunk/8.0.4/Data/Whitelistorblacklistspecificincomi ngdata "It is not necessary to define both an allow list and a deny list in a configuration stanza. The settings are independent. If you do define both filters and a file matches them both, Splunk Enterprise does not index that file, as the blacklist filter overrides the whitelist filter." Source:https://docs.splunk.com/Documentation/Splunk/8.1.0/Data/Whitelistorblacklistspecif icincomingdata

QUESTION 10

A Universal Forwarder is collecting two separate sources of data (A,B). Source A is being routed through a Heavy Forwarder and then to an indexer. Source B is being routed directly to the indexer. Both sets of data require the masking of raw text strings before being written to disk. What does the administrator need to do to ensure that the masking takes place successfully?

A. Make sure that props . conf and transforms . conf are both present on the in-dexer and the search head.

B. For source A, make sure that props . conf is in place on the indexer; and for source B, make sure transforms . conf is present on the Heavy Forwarder.

C. Make sure that props . conf and transforms . conf are both present on the Universal Forwarder.

D. Place both props . conf and transforms . conf on the Heavy Forwarder for source A, and place both props . conf and transforms . conf on the indexer for source B.

Correct Answer: D

The correct answer is D. Place both props . conf and transforms . conf on the Heavy Forwarder for source A, and place both props . conf and transforms . conf on the indexer for source B. According to the Splunk documentation1, to mask sensitive data from raw events, you need to use the SEDCMD attribute in the props.conf file and the REGEX attribute in the transforms.conf file. The SEDCMD attribute applies a sed expression to the raw data before indexing, while the REGEX attribute defines a regular expression to match the data to be masked.You need to place these files on the Splunk instance that parses the data, which isusually the indexer or the heavy forwarder2. The universal forwarder does not parse the data, so it does not need these files. For source A, the data is routed through a heavy forwarder, which can parse the data before sending it to the indexer. Therefore, you need to place both props.conf and transforms.conf on the heavy forwarder for source A, so that the masking takes place before indexing. For source B, the data is routed directly to the indexer, which parses and indexes the data. Therefore, you need to place both props.conf and transforms.conf on the indexer for source B, so that the masking takes place before indexing. References:1:Redact data from events - Splunk Documentation2:Where do I configure my Splunk settings? - Splunk Documentation

QUESTION 11

Which Splunk forwarder has a built-in license?

A. Light forwarder

B. Heavy forwarder

C. Universal forwarder

D. Cloud forwarder

Correct Answer: C

Reference:https://community.splunk.com/t5/Getting-Data-In/Do-we-need-a-license-for-Heavy-forwarder/m-p/210451

QUESTION 12

Where should apps be located on the deployment server that the clients pull from?

A. $SFLUNK_KOME/etc/apps

B. $SPLUNK_HCME/etc/sear:ch

C. $SPLUNK_HCME/etc/master-apps

D. $SPLUNK HCME/etc/deployment-apps

Correct Answer: D

After an app is downloaded, it resides under $SPLUNK_HOME/etc/apps on the deployment clients. But it resided in the $SPLUNK_HOME/etc/deployment-apps location in the deployment server.

QUESTION 13

What type of Splunk license is pre-selected in a brand new Splunk installation?

A. Free license

B. Forwarder license

C. Enterprise trial license

D. Enterprise license

Correct Answer: C

A Splunk Enterprise trial license gives you access to all the features of Splunk Enterprise for a limited period of time, usually 60 days1. After the trial period expires, you can either purchase a Splunk Enterprise license or switch to a Free license. A Splunk Enterprise Free license allows you to index up to 500 MB of data per day, but some features are disabled, such as authentication, distributed search, and alerting. You can switch to a Free license at any time during the trial period or after the trial period expires. A Splunk Enterprise Forwarder license is used with forwarders, which are Splunk instances that forward data to other Splunk instances. A Forwarder license does not allow indexing or searching of data. You can install a Forwarder license on any Splunk instance that you want to use as a forwarder. A Splunk Enterprise commercial end-user license is a license that you purchase from Splunk based on either data volume or infrastructure. This license gives you access to all the features of Splunk Enterprise within a defined limit of indexed data per day (volume-based license) or vCPU count (infrastructure license). You can purchase and install this license after the trial period expires or at any time during the trial period1.

QUESTION 14

If an update is made to an attribute in inputs.conf on a universal forwarder, on which Splunk component would the fishbucket need to be reset in order to reindex the data?

A. Indexer

B. Forwarder

C. Search head

D. Deployment server

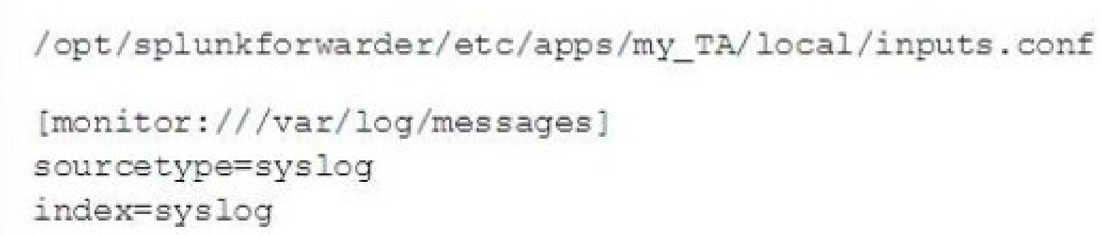
Correct Answer: A

https://www.splunk.com/en_us/blog/tips-and-tricks/what-is-this-fishbucket- thing.html "Every Splunk instance has a fishbucket index, except the lightest of hand-tuned lightweight forwarders, and if you index a lot of files it can get quite large. As any other index, you can change the retention policy to control the size via indexes.conf"

Reference https://community.splunk.com/t5/Archive/How-to-reindex-data-from-a- forwarder/td-p/93310

QUESTION 15

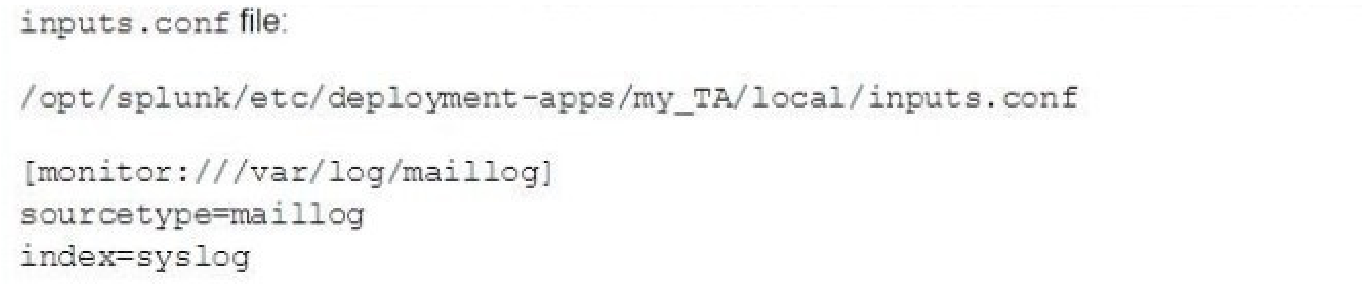
This file has been manually created on a universal forwarder



```
/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