Vendor: Splunk

Exam Code:SPLK-1003

Exam Name: Splunk Enterprise Certified Admin

Version: Demo

QUESTION 1

Which option accurately describes the purpose of the HTTP Event Collector (HEC)?

A. A token-based HTTP input that is secure and scalable and that requires the use of forwarders

B. A token-based HTTP input that is secure and scalable and that does not require the use of forwarders.

C. An agent-based HTTP input that is secure and scalable and that does not require the use of forwarders.

D. A token-based HTTP input that is insecure and non-scalable and that does not require the use of forwarders.

Correct Answer: B

https://docs.splunk.com/Documentation/Splunk/8.2.2/Data/UsetheHTTPEventCollector "The HTTP Event Collector (HEC) lets you send data and application events to a Splunk deployment over the HTTP and Secure HTTP (HTTPS) protocols. HEC uses a token- based authentication model. You can generate a token and then configure a logging library or HTTP client with the token to send data to HEC in a specific format. This process eliminates the need for a Splunk forwarder when you send application events."

QUESTION 2

When are knowledge bundles distributed to search peers?

A. After a user logs in.

B. When Splunk is restarted.

C. When adding a new search peer.

D. When a distributed search is initiated.

Correct Answer: D

"The search head replicates the knowledge bundle periodically in the background or when initiating a search. " "As part of the distributed search process, the search head replicates and distributes its knowledge objects to its search peers, or indexers. Knowledge objects include saved searches, event types, and other entities used in searching accorss indexes. The search head needs to distribute this material to its search peers so that they can properly execute queries on its behalf."

Reference: https://docs.splunk.com/Documentation/Splunk/8.0.5/DistSearch/Whatsearchheadssend

---

QUESTION 3

Which of the following enables compression for universal forwarders in outputs. conf ? A)

```
[udpout:mysplunk_indexer1]
compression=true
```

B)

```
[tcpout]
defaultGroup=my_indexers
compressed=true
```

C)

```
/opt/splunkforwarder/bin/splunk enable compression
```

D)

```
[tcpout:my_indexers] server=mysplunk_indexer1:9997, mysplunk_indexer2:9997
decompression=false
```

A. Option A

B. Option B

C. Option C

D. Option D

Correct Answer: B

https://docs.splunk.com/Documentation/Splunk/latest/Admin/Outputsconf

Compression # # This example sends compressed events to the remote indexer. # NOTE: Compression can be enabled TCP or SSL outputs only. # The receiver input port should also have compression enabled. [tcpout] server = splunkServer.example.com:4433 compressed = true

---

QUESTION 4

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 5

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

QUESTION 6

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 7

In which scenario would a Splunk Administrator want to enable data integrity check when creating an index?

A. To ensure that hot buckets are still open for writes and have not been forced to roll to a cold state

B. To ensure that configuration files have not been tampered with for auditing and/or legal purposes

C. To ensure that user passwords have not been tampered with for auditing and/or legal purposes.

D. To ensure that data has not been tampered with for auditing and/or legal purposes

Correct Answer: D

QUESTION 8

Which of the following applies only to Splunk index data integrity check?

A. Lookup table

B. Summary Index

C. Raw data in the index

D. Data model acceleration

Correct Answer: C

QUESTION 9

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/Usedefaultfieldssplunk_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 10

You update a props. conf file while Splunk is running. You do not restart Splunk and you run this command: splunk btoo1 props list --debug. What will the output be?

A. list of all the configurations on-disk that Splunk contains.

B. A verbose list of all configurations as they were when splunkd started.

C. A list of props. conf configurations as they are on-disk along with a file path from which the configuration is located

D. A list of the current running props, conf configurations along with a file path from which the configuration was made

Correct Answer: C

https://docs.splunk.com/Documentation/Splunk/8.0.1/Troubleshooting/Usebtooltotroublesh ootconfigurations

"The btool command simulates the merging process using the on-disk conf files and creates a report showing the merged settings."

"The report does not necessarily represent what\\'s loaded in memory. If a conf file change is made that requires a service restart, the btool report shows the change even though that change isn\\'t active."

QUESTION 11

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 12

On the deployment server, administrators can map clients to server classes using client filters. Which of the following statements is accurate?

A. The blacklist takes precedence over the whitelist.

B. The whitelist takes precedence over the blacklist.

C. Wildcards are not supported in any client filters.

D. Machine type filters are applied before the whitelist and blacklist.

Correct Answer: A

Reference: https://community.splunk.com/t5/Getting-Data-In/Can-I-use-both-the-whitelist-AND-blacklist-forthe-same/td-p/390910