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.certbus.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 of the following is a valid distributed search group?

A. [distributedSearch:Paris] default = false servers = server1, server2

B. [searchGroup:Paris] default = false servers = server1:8089, server2:8089

C. [searchGroup:Paris] default = false servers = server1:9997, server2:9997

D. [distributedSearch:Paris] default = false servers = server1:8089; server2:8089

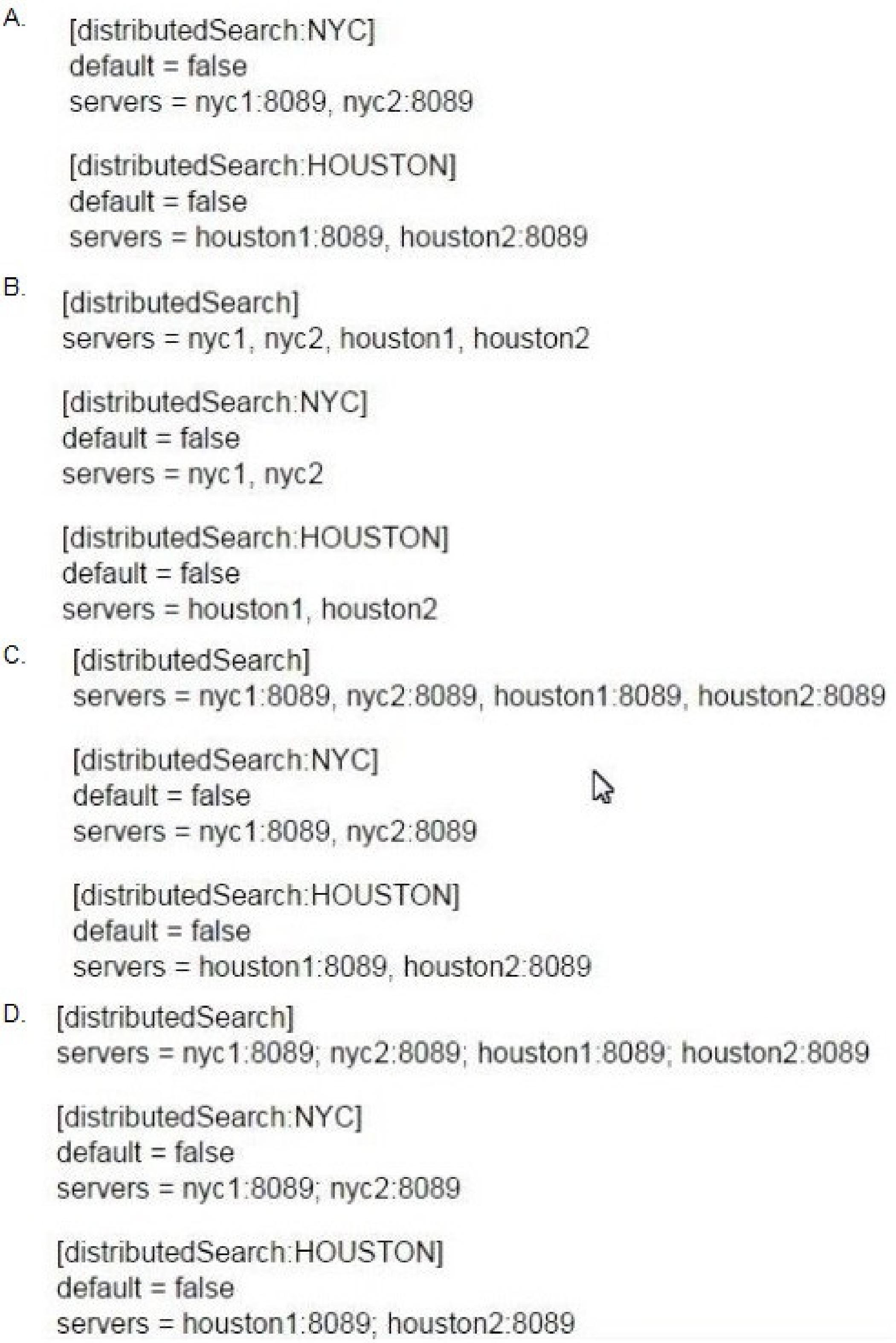
Correct Answer: D

https://docs.splunk.com/Documentation/Splunk/9.0.0/DistSearch/Distributedsearchgroups

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. Option A



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
```

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

What options are available when creating custom roles? (select all that apply)

A. Restrict search terms

B. Whitelist search terms

C. Limit the number of concurrent search jobs

D. Allow or restrict indexes that can be searched.

Correct Answer: ACD

https://docs.splunk.com/Documentation/SplunkCloud/8.2.2106/Admin/ConcurrentLimits "Set limits for concurrent scheduled searches. You must have the edit_search_concurrency_all and edit_search_concurrency_scheduled capabilities to configure these settings."

QUESTION 4

After configuring a universal forwarder to communicate with an indexer, which index can be checked via the Splunk Web UI for a successful connection?

A. index=main

B. index=test

C. index=summary

D. index=_internal

Correct Answer: D

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

QUESTION 5

When using license pools, volume allocations apply to which Splunk components?

A. Indexers

B. Indexes

C. Heavy Forwarders

D. Search Heads

Correct Answer: A

When using license pools, volume allocations apply to indexers. A license pool is a group of indexers that share a certain amount of daily indexing volume. The license pool specifies how much data each indexer can index per day, as well as which indexes are available for each indexer. Therefore, option A is the correct answer. References: Splunk Enterprise Certified Admin | Splunk, [Set up and manage license pools - Splunk Documentation]

QUESTION 6

In a customer managed Splunk Enterprise environment, what is the endpoint URI used to collect data?

A. services/collector

B. data/collector

C. services/inputs?raw

D. services/data/collector

Correct Answer: A

This is the endpoint URI used to collect data using the HTTP Event Collector (HEC), which is a token-based API that allows you to send data to Splunk Enterprise from any application that can make an HTTP request. The endpoint URI consists of the protocol (http or https), the hostname or IP address of the Splunk server, the port number (default is 8088), and the service name (services/collector). For example:
https://mysplunkserver.example.com:8088/services/collector

QUESTION 7

A company moves to a distributed architecture to meet the growing demand for the use of Splunk. What parameter can be configured to enable automatic load balancing in the

Universal Forwarder to send data to the indexers?

A. Create one outputs . conf file for each of the server addresses in the indexing tier.

B. Configure the outputs . conf file to point to any server in the indexing tier and Splunk will configure the data to be sent to all of the indexers.

C. Splunk does not do load balancing and requires a hardware load balancer to balance traffic across the indexers.

D. Set the stanza to have a server value equal to a comma-separated list of IP addresses and indexer ports for each of the indexers in the environment.

Correct Answer: D

Set the stanza to have a server value equal to a comma-separated list of IP addresses and indexer ports for each of the indexers in the environment. This is explained in the Splunk documentation, which states: To enable automatic load balancing, set the stanza to have a server value equal to a comma-separated list of IP addresses and indexer ports for each of the indexers in the environment. For example:

[tcpout] server=10.1.1.1:9997,10.1.1.2:9997,10.1.1.3:9997 The forwarder then distributes data across all of the indexers in the list.

QUESTION 8

Which Splunk component distributes apps and certain other configuration updates to search head cluster members?

A. Deployer

B. Cluster master

C. Deployment server

D. Search head cluster master

Correct Answer: C

https://docs.splunk.com/Documentation/Splunk/8.0.5/Updating/Updateconfigurations First line says it all: "The deployment server distributes deployment apps to clients."

QUESTION 9

What is the valid option for a [monitor] stanza in inputs.conf?

A. enabled

B. datasource

C. server_name

D. ignoreOlderThan

Correct Answer: D

Setting: ignoreOlderThan = Description: "Causes the input to stop checking files for updates if the file modification time has passed the threshold." Default: 0 (disabled)

QUESTION 10

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 11

In a customer managed Splunk Enterprise environment, what is the endpoint URI used to collect data?

A. services/ collector

B. services/ inputs ? raw

C. services/ data/ collector

D. data/ collector

Correct Answer: C

The answer to your question is C. services/data/collector. This is the endpoint URI used to collect data in a customer managed Splunk Enterprise environment.According to the Splunk documentation1, "The HTTP Event Collector REST API

endpoint is /services/data/collector.You can use this endpoint to send events to HTTP Event Collector on a Splunk Enterprise or Splunk Cloud Platform deployment." You can also use this endpoint to send events to a specific token or index1.

For example, you can use thefollowing curl command to send an event with the token 578254cc-05f5-46b5-957b-910d1400341a and the index main:

```
curl -k https://localhost:8088/services/data/collector -H\\'Authorization: Splunk 578254cc-
05f5-46b5-957b-910d1400341a\\'-d\\'{"index":"main","event":"Hello, world!"}\\'
```

QUESTION 12

Which forwarder type can parse data prior to forwarding?

A. Universal forwarder

B. Heaviest forwarder

C. Hyper forwarder

D. Heavy forwarder

Correct Answer: D

https://docs.splunk.com/Documentation/Splunk/latest/Forwarding/Typesofforwarders "A heavy forwarder parses data before forwarding it and can route data based on criteria such as source or type of event."

QUESTION 13

Which file will be matched for the following monitor stanza in inputs. conf?

[monitor: ///var/log/*/bar/*. txt]

A. /var/log/host_460352847/temp/bar/file/csv/foo.txt

B. /var/log/host_460352847/bar/foo.txt

C. /var/log/host_460352847/bar/file/foo.txt

D. /var/ log/ host_460352847/temp/bar/file/foo.txt

Correct Answer: C

The correct answer is C. /var/log/host_460352847/bar/file/foo.txt. The monitor stanza in inputs.conf is used to configure Splunk to monitor files and directories for new data.The monitor stanza has the following syntax1:

[monitor://]

The input path can be a file or a directory, and it can include wildcards (*) and regular expressions. The wildcards match any number of characters, including none, while the regular expressions match patterns of characters.The input path is

case-sensitive and must be enclosed in double quotes if it contains spaces1. In this case, the input path is /var/log//bar/.txt, which means Splunk will monitor any file with the .txt extension that is located in a subdirectory named bar under the /

var/log directory.The subdirectory bar can be at any level under the /var/log directory, and the * wildcard will match any characters before or after the bar and .txt parts1. Therefore, the file /var/log/host_460352847/bar/file/foo.txt will be

matched by the monitor stanza, as it meets the criteria. The other files will not be matched, because:

A. /var/log/host_460352847/temp/bar/file/csv/foo.txt has a .csv extension, not a .txt extension.

B. /var/log/host_460352847/bar/foo.txt is not located in a subdirectory under the bar directory, but directly in the bar directory. D. /var/log/host_460352847/temp/bar/file/foo.txt is located in a subdirectory named file under the bar directory, not directly in the bar directory.

QUESTION 14

Which Splunk component(s) would break a stream of syslog inputs into individual events? (select all that apply)

A. Universal Forwarder

B. Search head

C. Heavy Forwarder

D. Indexer

Correct Answer: CD

The correct answer is C and D. A heavy forwarder and an indexer are the Splunk components that can break a stream of syslog inputs into individual events. A universal forwarder is a lightweight agent that can forward data to a Splunk deployment, but it does not perform any parsing or indexing on the data. A search head is a Splunk component that handles search requests and distributes them to indexers, but it does not process incoming data. A heavy forwarder is a Splunk component that can perform parsing, filtering, routing, and aggregation on the data before forwarding it to indexers or other destinations.A heavy forwarder can break a stream of syslog inputs into individual events based on the line breaker and should linemerge settings in the inputs.conf file1. An indexer is a Splunk component that stores and indexes data, making it searchable.An indexer can also break a stream of syslog inputs into individual events based on the props.conf file settings, such as TIME_FORMAT, MAX_TIMESTAMP_LOOKAHEAD, and line_breaker2.

A Splunk component is a software process that performs a specific function in a Splunk deployment, such as data collection, data processing, data storage, data search, or data visualization. Syslog is a standard protocol for logging messages from network devices, such as routers, switches, firewalls, or servers. Syslog messages are typically sent over UDP or TCP to a central syslog server or a Splunk instance. Breaking a stream of syslog inputs into individual events means separating the data into discrete records that can be indexed and searched by Splunk. Each event should have a timestamp, a host, a source, and a sourcetype, which are the default fields that Splunk assigns to the data.
References:

1: Configure inputs using Splunk Connect for Syslog - Splunk Documentation

2: inputs.conf - Splunk Documentation

3: How to configure props.conf for proper line breaking ... - Splunk Community

4: Reliable syslog/tcp input ?splunk bundle style | Splunk

5: Configure inputs using Splunk Connect for Syslog - Splunk Documentation

6: About configuration files - Splunk Documentation [7]: Configure your OSSEC server to send data to the Splunk Add-on for OSSEC - Splunk Documentation [8]: Splunk components - Splunk Documentation [9]: Syslog - Wikipedia [10]: About default fields - Splunk Documentation

QUESTION 15

After how many warnings within a rolling 30-day period will a license violation occur with an enforced Enterprise license?

A. 1

B. 3

C. 4

D. 5

Correct Answer: D

https://docs.splunk.com/Documentation/Splunk/8.0.5/Admin/Aboutlicenseviolations "Enterprise Trial license. If you get five or more warnings in a rolling 30 days period, you are in violation of your license. Dev/Test license. If you generate five or more warnings in a rolling 30-day period, you are in violation of your license. Developer license. If you generate five or more warnings in a rolling 30-day period, you are in violation of your license. BUT for Free license. If you get three or more warnings in a rolling 30 days period, you are in violation of your license."

Reference: https://docs.splunk.com/Documentation/Splunk/8.0.5/Admin/Aboutlicenseviolations