Free Questions for SPLK-1003 by certsdeals

Shared by Howard on 12-12-2023

For More Free Questions and Preparation Resources

Check the Links on Last Page

Question 1

Question Type: MultipleChoice

A Universal Forwarder has the following active stanza in inputs . conf:

[monitor: //var/log]

disabled = O

host = 460352847

An event from this input has a timestamp of 10:55. What timezone will Splunk add to the event as part of indexing?

Options:

A- Universal Coordinated Time.

B- The timezone of the search head.

C- The timezone of the indexer that indexed the event.

D- The timezone of the forwarder.

Answer:

D

Explanation:

The correct answer is D. The timezone of the forwarder will be added to the event as part of indexing.

According to the Splunk documentation1, Splunk software determines the time zone to assign to a timestamp using the following logic in order of precedence:

Use the time zone specified in raw event data (for example, PST, -0800), if present.

Use the TZ attribute set in props.conf, if the event matches the host, source, or source type that the stanza specifies.

If the forwarder and the receiving indexer are version 6.0 or higher, use the time zone that the forwarder provides.

Use the time zone of the host that indexes the event.

In this case, the event does not have a time zone specified in the raw data, nor does it have a TZ attribute set in props.conf. Therefore, the next rule applies, which is to use the time zone that the forwarder provides. A universal forwarder is a lightweight agent that can forward data to a Splunk deployment, and it knows its system time zone and sends that information along with the events to the indexer2. The indexer then converts the event time to UTC and stores it in the _time field1.

The other options are incorrect because:

A) Universal Coordinated Time (UTC) is not the time zone that Splunk adds to the event as part of indexing, but rather the time zone that Splunk uses to store the event time in the _time field. Splunk software converts the event time to UTC based on the time zone that it determines from the rules above1.

B) The timezone of the search head is not relevant for indexing, as the search head is a Splunk component that handles search requests and distributes them to indexers, but it does not process incoming data3. The search head uses the user's timezone setting to determine the time range in UTC that should be searched and to display the timestamp of the results in the user's timezone2.

C) The timezone of the indexer that indexed the event is only used as a last resort, if none of the other rules apply. In this case, the forwarder provides the time zone information, so the indexer does not use its own time zone1.

Question 2

Question Type: MultipleChoice

Which pathway represents where a network input in Splunk might be found?

Options:

A- $SPLUNK HOME/ etc/ apps/ ne two r k/ inputs.conf

B- $SPLUNK HOME/ etc/ apps/ $appName/ local / inputs.conf

C- $SPLUNK HOME/ system/ local /udp.conf

D- $SPLUNK HOME/ var/lib/ splunk/$inputName/homePath/

Answer:

B

Explanation:

The correct answer is B. The network input in Splunk might be found in the $SPLUNK_HOME/etc/apps/$appName/local/inputs.conf file.

A network input is a type of input that monitors data from TCP or UDP ports. To configure a network input, you need to specify the port number, the connection host, the source, and the sourcetype in the inputs.conf file. You can also set other optional settings, such as index, queue, and host_regex1.

The inputs.conf file is a configuration file that contains the settings for different types of inputs, such as files, directories, scripts, network ports, and Windows event logs. The inputs.conf file can be located in various directories, depending on the scope and priority of the settings. The most common locations are:

$SPLUNK_HOME/etc/system/default: This directory contains the default settings for all inputs. You should not modify or copy the files in this directory2.

$SPLUNK_HOME/etc/system/local: This directory contains the custom settings for all inputs that apply to the entire Splunk instance. The settings in this directory override the default settings2.

$SPLUNK_HOME/etc/apps/$appName/default: This directory contains the default settings for all inputs that are specific to an app. You should not modify or copy the files in this directory2.

$SPLUNK_HOME/etc/apps/$appName/local: This directory contains the custom settings for all inputs that are specific to an app. The settings in this directory override the default and system settings2.

Therefore, the best practice is to create or edit the inputs.conf file in the $SPLUNK_HOME/etc/apps/$appName/local directory, where $appName is the name of the app that you want to configure the network input for. This way, you can avoid modifying the default files and ensure that your settings are applied to the specific app.

The other options are incorrect because:

A) There is no network directory under the apps directory. The network input settings should be in the inputs.conf file, not in a separate directory.

C) There is no udp.conf file in Splunk. The network input settings should be in the inputs.conf file, not in a separate file. The system directory is not the recommended location for custom settings, as it affects the entire Splunk instance.

D) The var/lib/splunk directory is where Splunk stores the indexed data, not the input settings. The homePath setting is used to specify the location of the index data, not the input data. The inputName is not a valid variable for inputs.conf.

Question 3

Question Type: **MultipleChoice**

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

Options:

A- Universal Forwarder

B- Search head

C- Heavy Forwarder

D- Indexer

Answer:

C, D

Explanation:

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 dat

a. 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.

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 4

Question Type: **MultipleChoice**

Syslog files are being monitored on a Heavy Forwarder.

Where would the appropriate TRANSFORMS setting be deployed to reroute logs based on the event message?

Options:

A- Heavy Forwarder

B- Indexer

C- Search head

D- Deployment server

Answer:

A

Explanation:

A Heavy Forwarder is a Splunk instance that can parse and filter data before forwarding it to another Splunk instance, such as an indexer1.A Heavy Forwarder can also perform index-time field extractions using the TRANSFORMS setting2.

The TRANSFORMS setting is used to configure data transformations in the transforms.conf file3.The transforms.conf file contains settings and values that you can use to configure host and source type overrides, anonymize sensitive data, route events to different indexes, create index-time and search-time field extractions, and set up lookup tables3.

The TRANSFORMS setting can be deployed to the Heavy Forwarder where the syslog files are being monitored, so that the logs can be rerouted based on the event message before they are forwarded to the indexer2.This can improve the performance and efficiency of data processing and indexing2.

Question 5

Question Type: MultipleChoice

Given a forwarder with the following outputs.conf configuration:

[tcpout : mypartner]

Server = 145.188.183.184:9097

[tcpout : hfbank]

server = inputsl . mysplunkhfs . corp : 9997 , inputs2 . mysplunkhfs . corp : 9997

Which of the following is a true statement?

Options:

A- Data will continue to flow to hfbank if 145.1 g a) 183.184 : 9097 is unreachable.

B- Data is not encrypted to mypartner because 145.188 .183.184 : 9097 is specified by IP.

C- Data is encrypted to mypartner because 145.183.184 : 9097 is specified by IP.

D- Data will eventually stop flowing everywhere if 145.188.183.184 : 9097 is unreachable.

Answer:

A

Explanation:

The outputs.conf file defines how forwarders send data to receivers1.You can specify some output configurations at installation time (Windows universal forwarders only) or the CLI, but most advanced configuration settings require that you edit outputs.conf1.

The [tcpout:...] stanza specifies a group of forwarding targets that receive data over TCP2.You can define multiple groups with different names and settings2.

The server setting lists one or more receiving hosts for the group, separated by commas2.If you specify multiple hosts, the forwarder load balances the data across them2.

Therefore, option A is correct, because the forwarder will send data to both inputsl.mysplunkhfs.corp:9997 and inputs2.mysplunkhfs.corp:9997, even if 145.188.183.184:9097 is unreachable.

Question 6

Question Type: **MultipleChoice**

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

A. Free license B. Forwarder license

Options:

C- Enterprise trial license

D- Enterprise license

Answer:

C

Explanation:

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 license1.

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 alerting2.You can switch to a Free license at any time during the trial period or after the trial period expires1.

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 data3.You can install a Forwarder license on any Splunk instance that you want to use as a forwarder4.

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 7

Question Type: MultipleChoice

Which of the following describes a Splunk deployment server?

Options:

A- A Splunk Forwarder that deploys data to multiple indexers.

B- A Splunk app installed on a Splunk Enterprise server.

C- A Splunk Enterprise server that distributes apps.

D- A server that automates the deployment of Splunk Enterprise to remote servers.

Answer:

C

Explanation:

A Splunk deployment server is a system that distributes apps, configurations, and other assets to groups of Splunk Enterprise instances.You can use it to distribute updates to most types of Splunk Enterprise components: forwarders, non-clustered indexers, and

search heads2.

A Splunk deployment server is available on every full Splunk Enterprise instance.To use it, you must activate it by placing at least one app into %SPLUNK_HOME%\etc\deployment-apps on the host you want to act as deployment server3.

A Splunk deployment server maintains the list of server classes and uses those server classes to determine what content to distribute to each client.A server class is a group of deployment clients that share one or more defined characteristics1.

A Splunk deployment client is a Splunk instance remotely configured by a deployment server. Deployment clients can be universal forwarders, heavy forwarders, indexers, or search heads.Each deployment client belongs to one or more server classes1.

A Splunk deployment app is a set of content (including configuration files) maintained on the deployment server and deployed as a unit to clients of a server class.A deployment app can be an existing Splunk Enterprise app or one developed solely to group some content for deployment purposes1.

Therefore, option C is correct, and the other options are incorrect.