Free Questions for SPLK-1003 by ebraindumps

Shared by Boone on 15-04-2024

For More Free Questions and Preparation Resources

Check the Links on Last Page

Question 1

Question Type: **MultipleChoice**

Immediately after installation, what will a Universal Forwarder do first?

Options:

A- Automatically detect any indexers in its subnet and begin routing data.

B- Begin reading local files on its server.

C- Begin generating internal Splunk logs.

D- Send an email to the operator that the installation process has completed.

Answer:

C

Explanation:

Begin generating internal Splunk logs.Immediately after installation, a Universal Forwarder will start generating internal Splunk logs that contain information about its own operation, such as startup and shutdown events, configuration changes, data ingestion, and forwarding activities1.These logs are stored in the$SPLUNK_HOME/var/log/splunkdirectory on the Universal Forwarder machine2.

Question 2

Question Type: **MultipleChoice**

A Splunk administrator has been tasked with developing a retention strategy to have frequently accessed data sets on SSD storage and to have older, less frequently accessed data on slower NAS storage. They have set a mount point for the NAS. Which parameter do they need to modify to set the path for the older, less frequently accessed data in indexes.conf?

Options:

A- homepath

B- thawedPath

C- summaryHomePath

D- colddeath

Answer:

D

Explanation:

The coldPath parameter defines the path for the cold buckets, which are the oldest and least frequently accessed data in an index1. By setting the coldPath to point to the NAS mount point, the Splunk administrator can achieve the retention strategy of having older data on slower NAS storage.

Question 3

Question Type: **MultipleChoice**

Which of the methods listed below supports muti-factor authentication?

Options:

A- Lightweight Directory Access Protocol (LDAP)

B- Security Assertion Markup Language (SAML)

C- Single Sign-on (SSO)

D- OpenlD

Answer:

B

Explanation:

SAML is an open standard for exchanging authentication and authorization data between parties, especially between an identity provider and a service provider1.SAML supports multi-factor authentication by allowing the identity provider to require the user to present two or more factors of evidence to prove their identity2. For example, the user may need to enter a password and a one-time code sent to their phone, or scan their fingerprint and face.

Question 4

Question Type: **MultipleChoice**

In inputs. conf, which stanza would mean Splunk was only reading one local file?

Options:

A- [read://opt/log/crashlog/Jan27crash.txt]

B- [monitor::/ opt/log/crashlog/Jan27crash.txt]

C- [monitor:/// opt/log/]

D- [monitor:/// opt/log/ crashlog/Jan27crash.txt]

Answer:

B

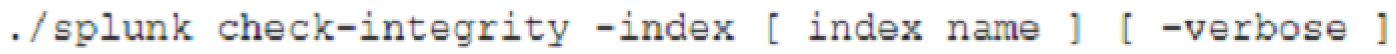
Explanation:

[monitor::/opt/log/crashlog/Jan27crash.txt].This stanza means that Splunk is monitoring a single local file named Jan27crash.txt in the /opt/log/crashlog/ directory1.The monitor input type is used to monitor files and directories for changes and index any new data that is added2.

Question 5

Question Type: **MultipleChoice**

When would the following command be used?



```
./splunk check-integrity -index [ index name ] [ -verbose ]
```

Options:

A- To verify' the integrity of a local index.

B- To verify the integrity of a SmartStore index.

C- To verify the integrity of a SmartStore bucket.

D- To verify the integrity of a local bucket.

Answer:

D

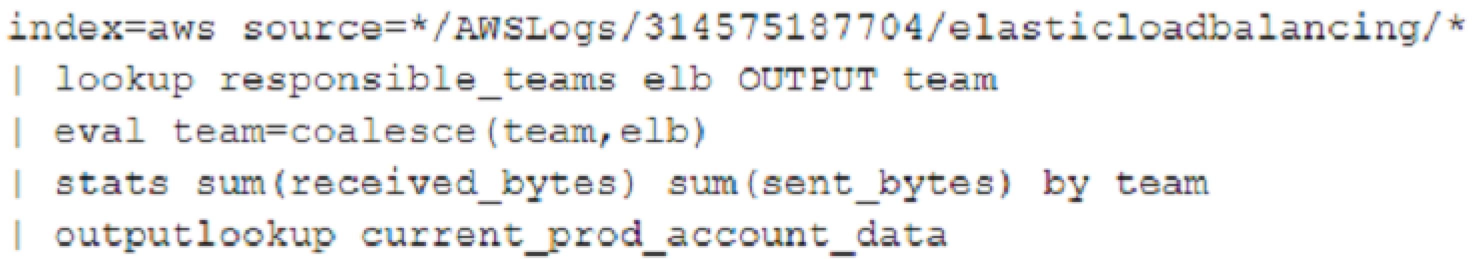
Explanation:

To verify the integrity of a local bucket.The command./splunk check-integrity -bucketPath [bucket path] [-verbose]is used to verify the integrity of a local bucket by comparing the hashes stored in the l1Hashes and l2Hash files with the actual data in the bucket1. This command can help detect any tampering or corruption of the data.

Question 6

Question Type: MultipleChoice

Running this search in a distributed environment:



```
index=aws source=*/AWSLogs/314575187704/elasticloadbalancing/*
| lookup responsible_teams elb OUTPUT team
| eval team=coalesce(team,elb)
| stats sum(received_bytes) sum(sent_bytes) by team
| outputlookup current_prod_account_data
```

On what Splunk component does the eval command get executed?

Options:

A- Heavy Forwarders

B- Universal Forwarders

C- Search peers

D- Search heads

Answer:

C

Explanation:

The eval command is a distributable streaming command, which means that it can run on the search peers in a distributed environment1.The search peers are the indexers that store the data and perform the initial steps of the search processing2.The eval command calculates an expression and puts the resulting value into a search results field1. In your search, you are using the eval command to create a new field called "responsible_team" based on the values in the "account" field.

Question 7

Question Type: MultipleChoice

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

Options:

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.

Answer:

A, C

Explanation:

The correct methods to connect a deployment client to a deployment server are A and C.You can either run the commandsplunk set deploy-poll <IP_address/hostname>:<management_port>from the command line of the deployment client1or create and edit a deploymentclient.conf file in$SPLUNK_HOME/etc/system/localon 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 8

Question Type: MultipleChoice

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?

Options:

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.

Answer:

D

Explanation:

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 documentation1, 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 9

Question Type: **MultipleChoice**

Which of the following types of data count against the license daily quota?

Options:

A- Replicated data

B- splunkd logs

C- Summary index data

D- Windows internal logs

Answer:

D

Explanation:

https://docs.splunk.com/Documentation/Splunk/8.0.3/Admin/Distdeploylicenses#Clustered_deployments_and_licensing_issues

Question 10

Question Type: MultipleChoice

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

Options:

A- Lookup table

B- Summary Index

C- Raw data in the index

D- Data model acceleration

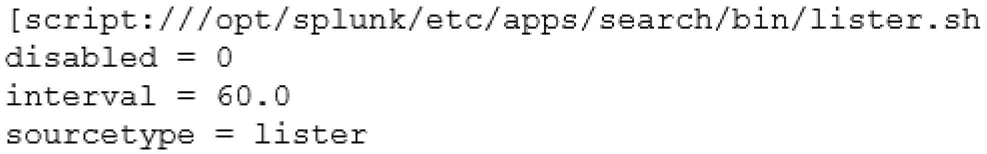
Answer:

C

Question 11

Question Type: **MultipleChoice**

Consider the following stanza in inputs.conf:



```
[script:///opt/splunk/etc/apps/search/bin/lister.sh
disabled = 0
interval = 60.0
sourcetype = lister
```

What will the value of the source filed be for events generated by this scripts input?

Options:

A- /opt/splunk/ecc/apps/search/bin/liscer.sh

B- unknown

C- liscer

D- liscer.sh

Answer:

A

Explanation:

https://docs.splunk.com/Documentation/Splunk/8.2.2/Admin/Inputsconf

-Scroll down to source = <string>

*Default: the input file path

To Get Premium Files for SPLK-1003 Visit

https://www.p2pexams.com/products/splk-1003

For More Free Questions Visit

https://www.p2pexams.com/splunk/pdf/splk-1003

20%
DISCOUNT