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.geekcert.com/splk-1003.html

100% Passing Guarantee
100% Money Back Assurance

Following Questions and Answers are all new published by Splunk Official Exam Center

- **Instant Download** After Purchase
- **100% Money Back** Guarantee
- **365 Days** Free Update
- **800,000+** Satisfied Customers

SATISFACTION GUARANTEED 100% SATISFACTION GUARANTEED

QUESTION 1

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 2

Where can scripts for scripted inputs reside on the host file system? (select all that apply)

A. $SFLUNK_HOME/bin/scripts

B. $SPLUNK_HOME/etc/apps/bin

C. $SPLUNK_HOME/etc/system/bin

D. $S?LUNK_HOME/etc/apps//bin_

Correct Answer: ACD

"Where to place the scripts for scripted inputs. The script that you refer to in $SCRIPT can reside in only one of the following places on the host file system: $SPLUNK_HOME/etc/system/bin $SPLUNK_HOME/etc/apps//bin $SPLUNK_HOME/bin/scripts As a best practice, put your script in the bin/ directory that is nearest to the inputs.conf file that calls your script on the host file system."

QUESTION 3

A new forwarder has been installed with a manually createddeploymentclient.conf.

What is the next step to enable the communication between the forwarder and the deployment server?

A. Restart Splunk on the deployment server.

B. Enable the deployment client in Splunk Web under Forwarder Management.

C. Restart Splunk on the deployment client.

D. Wait for up to the time set in thephoneHomeIntervalInSecssetting.

Correct Answer: C

The next step to enable the communication between the forwarder and the deployment server after installing a new forwarder with a manually created deploymentclient.conf is to restart Splunk on the deployment client. The deploymentclient.conf file contains the settings for the deployment client, which is a Splunk instance that receives updates from the deployment server. The file must include the targetUri attribute, which specifies the hostname and management port of the deployment server. To apply the changes in the deploymentclient.conf file, Splunk must be restarted on the deployment client. Therefore, option C is the correct answer. References: Splunk Enterprise Certified Admin | Splunk, [Configure deployment clients - Splunk Documentation]

QUESTION 4

What conf file needs to be edited to set up distributed search groups?

A. props.conf

B. search.conf

C. distsearch.conf

D. distibutedsearch.conf

Correct Answer: C

"You can group your search peers to facilitate searching on a subset of them. Groups of search peers are known as "distributed search groups." You specify distributed search groups in the distsearch.conf file"

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

QUESTION 5

When running a real-time search, search results are pulled from which Splunk component?

A. Heavy forwarders and search peers

B. Heavy forwarders

C. Search heads

D. Search peers

Correct Answer: D

Using the Splunk reference URLhttps://docs.splunk.com/Splexicon:Searchpeer

"search peer is a splunk platform instance that responds to search requests from a search head. The term "search peer" is usally synonymous with the indexer role in a distributed search topology. However, other instance types also have access to indexed data, particularly internal diagnostic data, and thus function as search peers when they respond to search requests for that data."

Latest SPLK-1003 Dumps SPLK-1003 VCE Dumps SPLK-1003 Practice Test