SPLK-1003Q&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.pass2lead.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

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

Which valid bucket types are searchable? (select all that apply)

A. Hot buckets

B. Cold buckets

C. Warm buckets

D. Frozen buckets

Correct Answer: ABC

Hot/warm/cold/thawed bucket types are searchable. Frozen isn\\'t searchable because its either deleted at that state or archived.

QUESTION 3

Which of the following are methods for adding inputs in Splunk? (select all that apply)

A. CLI

B. Splunk Web

C. Editing inputs. conf

D. Editing monitor. conf

Correct Answer: ABC

https://docs.splunk.com/Documentation/Splunk/8.2.2/Data/Configureyourinputs

Add your data to Splunk Enterprise. With Splunk Enterprise, you can add data using Splunk Web or Splunk Apps. In addition to these methods, you also can use the following methods. -The Splunk Command Line Interface (CLI) -The inputs.conf configuration file. When you specify your inputs with Splunk Web or the CLI, the details are saved in a configuartion file on Splunk Enterprise indexer and heavy forwarder instances.

QUESTION 4

During search time, which directory of configuration files has the highest precedence?

A. $SFLUNK_KOME/etc/system/local

B. $SPLUNK_KCME/etc/system/default

C. $SPLUNK_HCME/etc/apps/app1/local

D. $SPLUNK HCME/etc/users/admin/local

Correct Answer: D

Adding further clarity and quoting same Splunk reference URL from @giubal"

"To keep configuration settings consistent across peer nodes, configuration files are managed from the cluster master, which pushes the files to the slave-app directories on the peer nodes. Files in the slave-app directories have the highest precedence in a cluster peer\\'s configuration. Here is the expanded precedence order for cluster peers: 1.Slave-app local directories -- highest priority

2.

System local directory

3.

App local directories

4.

Slave-app default directories

5.

App default directories

6.

System default directory --lowest priority

QUESTION 5

Which of the following is the use case for the deployment server feature of Splunk?

A. Managing distributed workloads in a Splunk environment.

B. Automating upgrades of Splunk forwarder installations on endpoints.

C. Orchestrating the operations and scale of a containerized Splunk deployment.

D. Updating configuration and distributing apps to processing components, primarily forwarders.

Correct Answer: D

https://docs.splunk.com/Documentation/Splunk/8.2.2/Updating/Aboutdeploymentserver

"The deployment server is the tool for distributing configurations, apps, and content updates to groups of Splunk Enterprise instances."