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.pass4itsure.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 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 2

Using the CLI on the forwarder, how could the current forwarder to indexer configuration be viewed?

A. splunk btool server list --debug

B. splunk list forward-indexer

C. splunk list forward-server

D. splunk btool indexes list --debug

Correct Answer: C

Reference:https://community.splunk.com/t5/All-Apps-and-Add-ons/How-do-I-configure-a- Splunk-Forwarder-on-Linux/m-p/72078 The CLI command to view the current forwarder to indexer configuration is splunk list forward-server. This command displays the hostnames and port numbers of the indexers that the forwarder sends data to. Therefore, option C is the correct answer. References: Splunk Enterprise Certified Admin | Splunk, [Use CLI commands to manage your forwarders - Splunk Documentation]

QUESTION 3

In which phase do indexed extractions in props.conf occur?

A. Inputs phase

B. Parsing phase

C. Indexing phase

D. Searching phase

Correct Answer: B

The following items in the phases below are listed in the order Splunk applies them (ie LINE_BREAKER occurs before TRUNCATE).

Input phase inputs.conf props.conf CHARSET NO_BINARY_CHECK CHECK_METHOD CHECK_FOR_HEADER (deprecated) PREFIX_SOURCETYPE sourcetype wmi.conf regmon-filters.conf Structured parsing phase props.conf INDEXED_EXTRACTIONS, and all other structured data header extractions Parsing phase props.conf LINE_BREAKER, TRUNCATE, SHOULD_LINEMERGE, BREAK_ONLY_BEFORE_DATE, and all other line merging settings TIME_PREFIX, TIME_FORMAT, DATETIME_CONFIG (datetime.xml), TZ, and all other time extraction settings and rules TRANSFORMS which includes per-event queue filtering, per-event index assignment, per- event routing SEDCMD MORE_THAN, LESS_THAN transforms.conf stanzas referenced by a TRANSFORMS clause in props.conf LOOKAHEAD, DEST_KEY, WRITE_META, DEFAULT_VALUE, REPEAT_MATCH

QUESTION 4

How can native authentication be disabled in Splunk?

A. Remove the $SPLUNK_HOME/etc/passwd file

B. Create an empty $SPLUNK_HOME/etc/passwd file

C. Set SPLUNK_AUTHENTICATION=false in splunk-launch.conf

D. Set nativeAuthentication=false in authentication.conf

Correct Answer: B

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

QUESTION 5

The volume of data from collecting log files from 50 Linux servers and 200 Windows servers will require multiple indexers. Following best practices, which types of Splunk component instances are needed?

A. Indexers, search head, universal forwarders, license master

B. Indexers, search head, deployment server, universal forwarders

C. Indexers, search head, deployment server, license master, universal forwarder

D. Indexers, search head, deployment server, license master, universal forwarder, heavy forwarder

Correct Answer: C

Indexers, search head, deployment server, license master, universal forwarder. This is the combination of Splunk component instances that are needed to handle the volume of data from collecting log files from 50 Linux servers and 200 Windows servers, following the best practices. The roles and functions of these components are: Indexers: These are the Splunk instances that index the data and make it searchable. They also perform some data processing, such as timestamp extraction, line breaking, and field extraction. Multiple indexers can be clustered together to provide high availability, data replication, and load balancing. Search head: This is the Splunk instance that coordinates the search across the indexers and merges the results from them. It also provides the user interface for searching, reporting, and dashboarding. A search head can also be clustered with other search heads to provide high availability, scalability, and

load balancing. Deployment server: This is the Splunk instance that manages the configuration and app deployment for the universal forwarders. It allows the administrator to centrally control the inputs.conf, outputs.conf, and other configuration files for the forwarders, as well as distribute apps and updates to them. License master: This is the Splunk instance that manages the licensing for the entire Splunk deployment. It tracks the license usage of all the Splunk instances and enforces the license limits and violations. It also allows the administrator to add, remove, or change licenses. Universal forwarder: These are the lightweight Splunk instances that collect data from various sources and forward it to the indexers or other forwarders. They do not index or parse the data, but only perform minimal processing, such as compression and encryption. They are installed on the Linux and Windows servers that generate the log files.