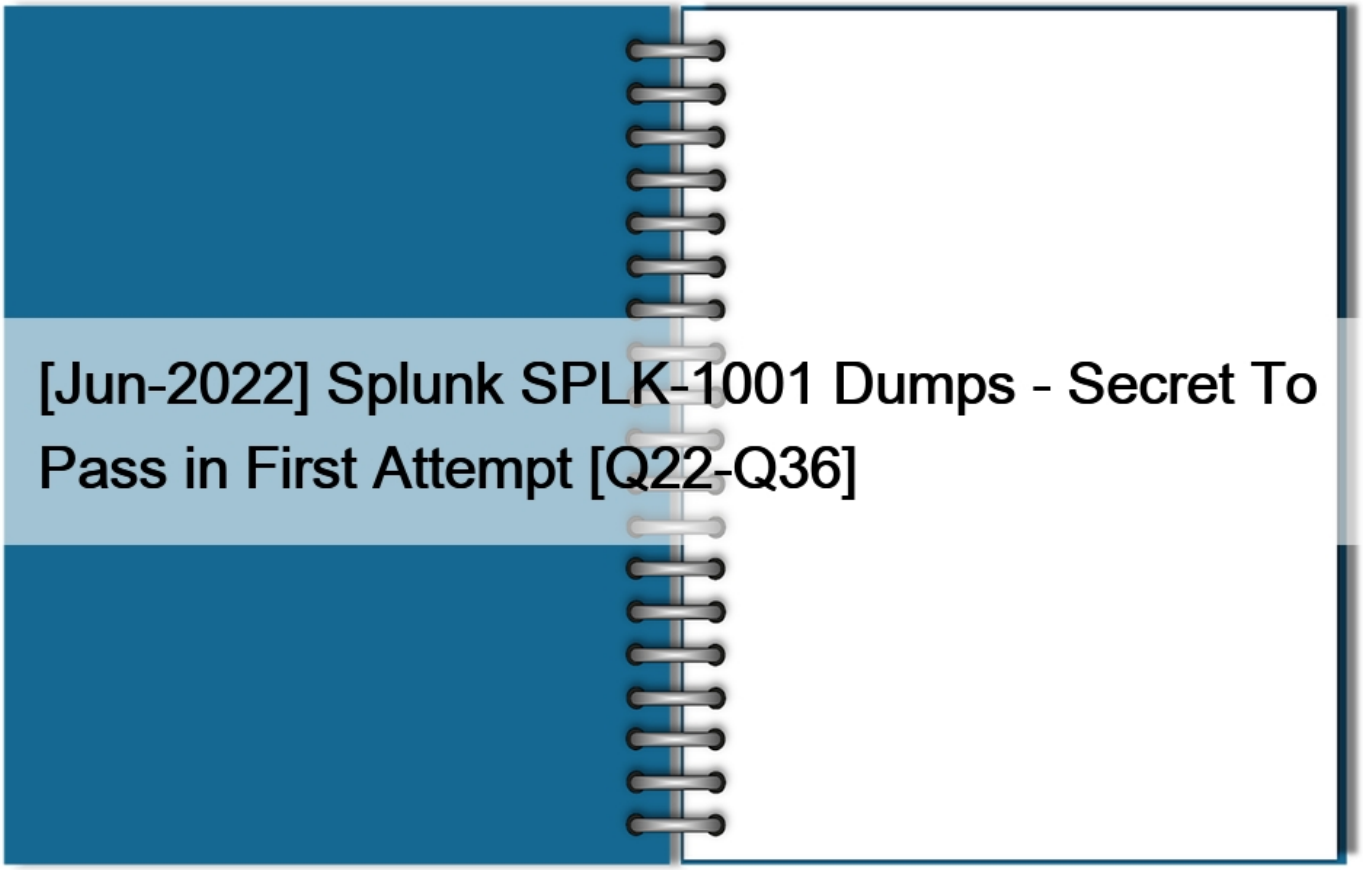
[Jun-2022 Splunk SPLK-1001 Dumps - Secret To Pass in First Attempt [Q22-Q36



[Jun-2022] Splunk SPLK-1001 Dumps - Secret To Pass in First Attempt
Splunk SPLK-1001 Exam Dumps [2022] Practice Valid Exam Dumps Question

Sample Questions

Which Splunk component receives, indexes, and stores incoming data from forwarders?
- Cluster master- Indexer- Search head- Deployment server

Which license type allows 500MB/day of indexing, but disables alerts, authentication, cluster, distributed search, summarization, and forwarding to non-Splunk servers?
- Forwarder license- Free license- Enterprise trial license- Enterprise license

What can be used when setting the host field option on a network input? (select all that apply)
- Custom (explicit value)- DNS- A binary file- IP

By default, all users have DELETE permission to ALL knowledge objects.
- True- False

Which stats command function provides a count of how many unique values exist for a given field in the result set?
- distinct-count(field)- count-by(field)- count(field)- dc(field)

A collection of items containing things such as data inputs, UI elements, and knowledge objects is known as what?
- A role- An app- JSON

How to Prepare for Splunk Core Certified User (SPLK-1001) **Preparation Guide for Splunk Core Certified User (SPLK-1001) Introduction for Splunk Core Certified User (SPLK-1001)**

Splunk has created a track for IT professionals to certify as a Certified Power User on the Splunk platform. This certification program provides Splunk professionals with a way to demonstrate their skills. The assessment is based on a rigorous exam using the industry-standard methodology to determine whether a candidate meets Splunk's proficiency standards.

A Splunk Core Certified User is able to search, use fields, create alerts, use look-ups, and create basic statistical reports and dashboards in either the Splunk Enterprise or Splunk Cloud platforms. This optional entry-level certification demonstrates an individual's basic ability to navigate and use Splunk software.

A certified Admin manages various components of Splunk Enterprise on a daily basis, including license management, indexers and search heads, configuration, monitoring, and getting data into Splunk. This certification demonstrates an individual's ability to support the day-to-day administration and health of a Splunk Enterprise environment.

The Splunk Enterprise System Administration course focuses on administrators who manage a Splunk Enterprise environment. Topics include Splunk license manager, indexers and search heads, configuration, management, and monitoring. The Splunk Enterprise Data Administration course targets administrators who are responsible for getting data into Splunk. The course provides content about Splunk forwarders and methods to get remote data into Splunk.

In this guide, we will cover the Splunk Core Certified User (SPLK-1001), tips and tricks, salary, certififcation path and also share the benefits of **SPLUNK SPLK-1001 practice exam** and **SPLUNK SPLK-1001 practice exams**.

Do you want to declare a statement of intent and design a statistical report through certification training? If so, you need to enroll in the Splunk SPLK-1001 exam.

NO.22 Which of the following are functions of the stats command?
* count, sum, add
* count, sum, less
* sum, avg. values
* sum, values, table

NO.23 The command shown here does witch of the following: Command: |outputlookup products.csv
* Writes search results to a file named products.csv
* Returns the contents of a file named products.csv

NO.24 Which search will return the 15 least common field values for the dest_ip field?
* sourcetype=firewall | rare num=15 dest_ip
* sourcetype=firewall | rare last=15 dest_ip
* sourcetype=firewall | rare count=15 dest_ip
* sourcetype=firewall | rare limit=15 dest_ip

NO.25 What are the steps to schedule a report?
* After saving the report, click Schedule
* After saving the report, click Event Type
* After saving the report, click Scheduling
* After saving the report, click Dashboard Panel

NO.26 Which of the following searches will show the number of categoryld used by each host?
* Sourcetype=access_* |sum bytes by host
* Sourcetype=access_* |stats sum(categorylD. by host
* Sourcetype=access_* |sum(bytes) by host
* Sourcetype=access_* |stats sum by host

NO.27 What is a quick, comprehensive way to learn what data is present in a Splunk deployment?
* Review Splunk reports
* Run ./splunk show
* Click Data Summary in Splunk Web
* Search index=* sourcetype=* host=*

Explanation/Reference: https://docs.splunk.com/Documentation/Splunk/8.0.3/InheritedDeployment/Yourdata

NO.28 Monitor option in Add Data provides _____.
* Only continuous monitoring.
* Only One-time monitoring.
* None of the above.
* Both One-time and continuous monitoring

NO.29 Following are the time selection option while making search:

(Choose all that apply.)
* Date & Time Range
* Advanced
* Date Range
* Presets
* Relative

NO.30 What does the stats command do?
* Automatically correlates related fields
* Converts field values into numerical values
* Calculates statistics on data that matches the search criteria
* Analyzes numerical fields for their ability to predict another discrete field

NO.31 What options do you get after selecting timeline? (Choose four.)
* Zoom to selection
* Format Timeline
* Deselect
* Delete
* Zoom Out

NO.32 Put query into separate lines where | (Pipes) are used by selecting following options.
* CTRL + Enter
* Shift + Enter
* Space + Enter
* ALT + Enter

NO.33 Which of the following is a best practice when writing a search string?
* Include all formatting commands before any search terms
* Include at least one function as this is a search requirement
* Include the search terms at the beginning of the search string
* Avoid using formatting clauses as they add too much overhead

NO.34 When running searches, command modifiers in the search string are displayed in what color?
* Red

* Blue
* Orange
* Highlighted

Explanation/Reference: https://docs.splunk.com/Documentation/Splunk/7.2.6/Search/Parsingsearches

NO.35 Splunk extracts fields from event data at index time and at search time.

* True
* False

NO.36 After running a search, what effect does clicking and dragging across the timeline have?

* Executes a new search.
* Filters current search results.
* Moves to past or future events.
* Expands the time range of the search.

Explanation

Explanation/Reference: https://docs.splunk.com/Documentation/Splunk/7.2.6/Search/Usethetimeline

SPLK-1001 Exam Dumps PDF Guaranteed Success with Accurate & Updated Questions:
https://www.examslabs.com/Splunk/Splunk-Core-Certified-User/best-SPLK-1001-exam-dumps.html]