

SPLK-1003 Actual Braindumps & SPLK-1003 Latest Version



BTW, DOWNLOAD part of Easy4Engine SPLK-1003 dumps from Cloud Storage: https://drive.google.com/open?id=1KX2kfHGwgk8lR2kjZy4MKf19I_oStuB_

Many clients may worry that if they buy our product they will fail in the exam but we guarantee to you that our SPLK-1003 study questions are of high quality and can help you pass the exam easily and successfully. Our product boasts 99% passing rate and high hit rate so you needn't worry that you can't pass the exam. Our SPLK-1003 exam torrent is compiled by experts and approved by experienced professionals and updated according to the development situation in the theory and the practice. Our Splunk Enterprise Certified Admin guide torrent can simulate the exam and boosts the timing function. The language is easy to be understood and makes the learners have no learning obstacles. So our SPLK-1003 Exam Torrent can help you pass the exam with high possibility.

The SPLK-1003 certification exam is a performance-based exam that requires candidates to demonstrate their practical knowledge and skills in administering Splunk Enterprise environments. SPLK-1003 exam covers a range of topics, including installation and configuration, data inputs and forwarders, search and reporting, user management, and monitoring and troubleshooting. SPLK-1003 exam is designed to test the candidate's ability to deploy and manage Splunk Enterprise environments in a variety of scenarios.

Understanding functional and technical aspects of Splunk Enterprise Certified Admin Basics and License Management

The following will be discussed in **SPLUNK SPLK-1003 Exam Dumps Pdf**:

- Understand license violations
- Identify Splunk components
- Identify license types

Choose Updated Splunk SPLK-1003 Preparation Material in 3 Formats

Easy4Engine provide people a relatively short period of time with a great important SPLK-1003 Exam tool to pass the qualification test. If someone choose the our high efficiency exam tool, our reliable SPLK-1003 dump can help users quickly analysis in the difficult point, high efficiency of review, and high quality through the exam, work for our future employment and increase the weight of the promotion, to better meet the needs of their own development.

Splunk Enterprise Certified Admin Sample Questions (Q181-Q186):

NEW QUESTION # 181

Which data pipeline phase is the last opportunity for defining event boundaries?

- A. Indexing phase
- B. Input phase
- C. Parsing phase
- D. Search phase

Answer: C

Explanation:

Explanation

Reference: <https://docs.splunk.com/Documentation/Splunk/8.2.3/Admin/Configurationparametersandthedatapipeline> The parsing phase is the process of extracting fields and values from raw data. The parsing phase respects LINE_BREAKER, SHOULD_LINEMERGE, BREAK_ONLY_BEFORE_DATE, and all other line merging settings in props.conf. These settings determine how Splunk breaks the data into events based on certain criteria, such as timestamps or regular expressions. The event boundaries are defined by the props.conf file, which can be modified by the administrator. Therefore, the parsing phase is the last opportunity for defining event boundaries.

NEW QUESTION # 182

An add-on has configured field aliases for source IP address and destination IP address fields. A specific user prefers not to have those fields present in their user context. Based on the default props.conf below, which SPLUNK_HOME/etc/users/buttercup/myTA/local/props.conf stanza can be added to the user's local context to disable the field aliases?

```
SPLUNK_HOME/etc/apps/myTA/default/props.conf
[mySourcetype]
FIELDALIAS-cim-src_ip = sourceIPAddress as src_ip
FIELDALIAS-cim-dest_ip = destinationIPAddress as dest_ip
```

```

A. [mySourcetype]
   disable FIELDALIAS-cim-src_ip
   disable FIELDALIAS-cim-dest-ip

B. [mySourcetype]
   FIELDALIAS-cim-src_ip =
   FIELDALIAS-cim-dest-ip =

C. [mySourcetype]
   unset FIELDALIAS-cim-src_ip
   unset FIELDALIAS-cim-dest-ip

D. [mySourcetype]
   #FIELDALIAS-cim-src_ip = sourceIPAddress as src_ip
   #FIELDALIAS-cim-dest-ip = destinationIPAddress as dest_ip

```

- A. Option D
- **B. Option B**
- C. Option A
- D. Option C

Answer: B

NEW QUESTION # 183

Assume a file is being monitored and the data was incorrectly indexed to an exclusive index. The index is cleaned and now the data must be reindexed. What other index must be cleaned to reset the input checkpoint information for that file?

- A. `_checkpoint`
- B. `_audit`
- C. `_introspection`
- **D. `_thefishbucket`**

Answer: D

Explanation:

--reset Reset the fishbucket for the given key or file in the btree. Resetting the checkpoint for an active monitor input reindexes data, resulting in increased license use. <https://docs.splunk.com/Documentation/Splunk/8.1.1/Troubleshooting/CommandlinetoolsforusewithSupport>

NEW QUESTION # 184

What action is required to enable forwarder management in Splunk Web?

- A. Navigate to Settings > Forwarding and receiving, and click on Enable Forwarding.
- B. Navigate to Settings > Server Settings > General Settings, and set an App server port.
- **C. Create a server class and map it to a client in `SPLUNK_HOME/etc/system/local/serverclass.conf`.**
- D. Place an app in the `SPLUNK_HOME/etc/deployment-apps` directory of the deployment server.

Answer: C

Explanation:

Reference:

<https://docs.splunk.com/Documentation/MSApp/2.0.3/MSInfra/Setupadeploymentserver>

"To activate deployment server, you must place at least one app into `%SPLUNK_HOME%\etc\deployment-apps` on the host you

BONUS!!! Download part of Easy4Engine SPLK-1003 dumps for free: https://drive.google.com/open?id=1KX2kfHGwgk8lR2kjZy4MKf19l_oSluB_