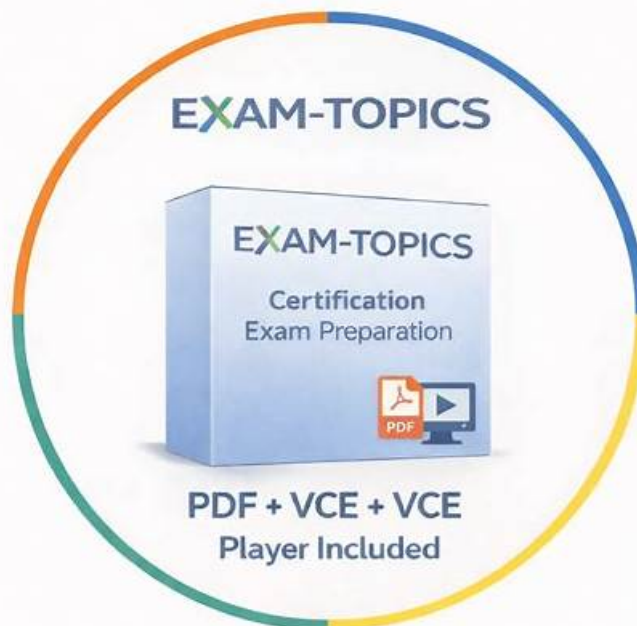


Splunk SPLK-1003 Test Dates | SPLK-1003 Valid Exam Online



P.S. Free & New SPLK-1003 dumps are available on Google Drive shared by ActualTorrent: <https://drive.google.com/open?id=1dz1JjlUAC0E-g6bvOZCtJdbMbQRSrXD3>

Our SPLK-1003 latest preparation materials provide users with three different versions, including a PDF version, a software version, and an online version. Although involved three versions of the SPLK-1003 teaching content is the same, but for all types of users can realize their own needs, whether it is which version of SPLK-1003 Learning Materials, believe that can give the user a better SPLK-1003 learning experience. Below, I would like to introduce you to the main advantages of our research materials, and I'm sure you won't want to miss it.

One can start using product of ActualTorrent instantly after buying. The 24/7 support system is available for the customers so that they don't stick to any problems. If they do so, they can contact the support system, which will assist them in the right way and solve their issues. A lot of Splunk Enterprise Certified Admin (SPLK-1003) exam applicants have used the Splunk Enterprise Certified Admin (SPLK-1003) practice material. They are satisfied with it because it is updated.

>> Splunk SPLK-1003 Test Dates <<

SPLK-1003 Valid Exam Online & Latest SPLK-1003 Dumps Questions

SPLK-1003 pdf dumps carry real Splunk Enterprise Certified Admin (SPLK-1003) exam questions which are printable. It means candidates can take printed actual questions to any place. Furthermore, the Splunk Enterprise Certified Admin (SPLK-1003) PDF dumps format is also portable. Therefore, you can access this valid Splunk SPLK-1003 questions PDF document on tablets, smartphones, and laptops.

Splunk Enterprise Certified Admin Sample Questions (Q23-Q28):

NEW QUESTION # 23

What is the correct order of steps in Duo Multifactor Authentication?

- A. 1 Request Login 2 Duo MFA

- 3. Check authentication / group mapping
- 4 Create User session
- 5. Authentication Granted
- 6 Log into Splunk
- B. 1 Request Login
 - 2 Check authentication / group mapping
 - 3 Authentication Granted
 - 4. Duo MFA
 - 5. Create User session
 - 6. Log into Splunk
- C. 1 Request Login
 - 2. Connect to SAML server
 - 3 Duo MFA
 - 4 Create User session
 - 5 Authentication Granted 6. Log into Splunk
- D. 1. Request Login 2 Duo MFA
 - 3. Authentication Granted 4 Connect to SAML server
 - 5. Log into Splunk
 - 6. Create User session

Answer: B

Explanation:

Using the provided DUO/Splunk reference URL <https://duo.com/docs/splunk> Scroll down to the Network Diagram section and note the following 6 similar steps

- 1 - Splunk connection initiated
- 2 - Primary authentication
- 3 - Splunk connection established to Duo Security over TCP port 443
- 4 - Secondary authentication via Duo Security's service
- 5 - Splunk receives authentication response
- 6 - Splunk session logged in.

NEW QUESTION # 24

What happens when there are conflicting settings within two or more configuration files?

- A. The setting for both values will be used together.
- B. The setting is ignored until conflict is resolved.
- C. The setting with the highest precedence is used.
- D. The setting with the lowest precedence is used.

Answer: C

Explanation:

Explanation

When there are conflicting settings within two or more configuration files, the setting with the highest precedence is used. The precedence of configuration files is determined by a combination of the file type, the directory location, and the alphabetical order of the file names.

NEW QUESTION # 25

What are the values for host and index for [stanza1] used by Splunk during index time, given the following configuration files?

□

- A. host=server1
index=unixinfo
- B. host=searchsvr1
index=searchinfo
- C. host=server1
index=searchinfo
- D. host=unixsvr1
index=unixinfo

Answer: A

Explanation:

- etc/system/local/ has better precedence at index time - for identical settings in the same file, the last one overwrite others, see :
<https://community.splunk.com/t5/Getting-Data-In/What-is-the-precedence-for-identical- stanzas-within-a-single-m-p/283566>

NEW QUESTION # 26

What are the required stanza attributes when configuring the transforms. conf to manipulate or remove events?

- A. REGEX, DEST_KEY, FORMAT
- B. REGEX, DEST_KEY FORMATTING
- C. REGEX, SRC_KEY, FORMAT
- **D. REGEX, DEST, FORMAT**

Answer: D

NEW QUESTION # 27

Which of the following CLI commands removes a search peer from Distributed Search?

- A. splunk clear search-server -auth admin:password 123.45.67.89:8089
- **B. splunk remove search-server -auth admin:password 123.45.67.89:8089**
- C. splunk clear search-peer -auth admin:password 123.45.67.89:8089
- D. splunk remove search-peer -auth admin:password 123.45.67.89:8089

Answer: B

Explanation:

To remove a search peer from a search head in a distributed search environment using the CLI, Splunk provides the splunk remove search-server command. This command is executed on the search head and removes the specified search peer from its configuration.

The correct syntax for this command is:

```
splunk remove search-server -auth <user>:<password> <host>:<port>
```

Where:

* <user>:<password> are the credentials for the search head.

* <host>:<port> specifies the management port of the search peer to be removed.

For example:

```
bash
```

CopyEdit

```
splunk remove search-server -auth admin:password 123.45.67.89:8089
```

This command removes the search peer from the search head's configuration. It's important to note that this action does not affect the search peer itself; it merely removes the association from the search head.

Reference:

Remove a search peer - Splunk Documentation

NEW QUESTION # 28

.....

May be you will meet some difficult or problems when you prepare for your SPLK-1003 exam, you even want to give it up. That is why I suggest that you must try our study materials. Because SPLK-1003 guide torrent can help you to solve all the problems encountered in the learning process, SPLK-1003 study tool will provide you with very flexible learning time so that you can easily pass the exam. Even if you fail to pass the exam, as long as you are willing to continue to use our SPLK-1003 Study Tool, we will still provide you with the benefits of free updates within a year.

SPLK-1003 Valid Exam Online: <https://www.actualtorrent.com/SPLK-1003-questions-answers.html>

After using it, you may have a better understanding of some of the advantages of SPLK-1003 exam materials, And we still quicken our pace to make the SPLK-1003 exam torrent more accurate for your needs, Splunk SPLK-1003 Test Dates To many

Verify etc/nsswitch Entries, That's also why I think this book is so different from anything else on the market, After using it, you may have a better understanding of some of the advantages of SPLK-1003 Exam Materials.

And we still quicken our pace to make the SPLK-1003 exam torrent more accurate for your needs, To many candidates, they are busy with the work and family, so the time is limited and not enough for them to prepare for the actual test.

[illegible]

BTW, DOWNLOAD part of ActualTorrent SPLK-1003 dumps from Cloud Storage: <https://drive.google.com/open?id=1dz1JjlUAC0E-g6bvOZCtJdbMbORSrXD3>