

Pass Guaranteed Splunk - Accurate Valid SPLK-1003 Exam Review



BONUS!!! Download part of Getcertkey SPLK-1003 dumps for free: <https://drive.google.com/open?id=1hbbRsvBLEzIPX1mfpZtd2Sfcus9WS2>

The opportunity always belongs to a person who has the preparation. But, when opportunities arise, will you seize the opportunities successfully? At present, you are preparing for Splunk SPLK-1003 test. Will you seize Getcertkey to make you achievement? Getcertkey Splunk SPLK-1003 certification training materials will guarantee your success. With our exam preparation materials, you will save a lot of time and pass your exam effectively. If you choose Getcertkey study guide, you will find the test questions and test answers are certainly different and high-quality, which is the royal road to success. And then, the dumps will help you prepare well enough for SPLK-1003 Exam.

With many advantages such as immediate download, simulation before the real exam as well as high degree of privacy, our SPLK-1003 actual exam survives all the ordeals throughout its development and remains one of the best choices for those in preparation for SPLK-1003 Exam. Many people have gained good grades after using our SPLK-1003 real dumps, so you will also enjoy the good results. Don't hesitate any more. Time and tide wait for no man. Come and buy our SPLK-1003 exam questions!

>> Valid SPLK-1003 Exam Review <<

Don't Miss Up to 1 year of Free Updates – Buy Splunk SPLK-1003 Dumps Now

The Getcertkey SPLK-1003 exam questions are checked and verified by experienced and qualified Splunk Enterprise Certified Admin exam trainers. So you can trust on the validity and top standard of Getcertkey SPLK-1003 exam practice test questions.

With the Getcertkey SPLK-1003 exam questions you will get everything that you need to prepare and pass the challenging Splunk SPLK-1003 Exam with good scores. The Getcertkey SPLK-1003 exam questions will give you an idea about the final SPLK-1003 exam format and you will get experience about SPLK-1003 exam format before the final exam.

The SPLK-1003 exam is aimed at IT professionals who have experience working with and administering Splunk Enterprise. SPLK-1003 exam is intended for candidates who are comfortable with the basic concepts and terminology of Splunk and have a good understanding of the Splunk search language. SPLK-1003 Exam is also appropriate for those who have completed the Splunk Fundamentals 1 and 2 courses, as well as the Splunk Administrator course.

Splunk Enterprise Certified Admin Sample Questions (Q135-Q140):

NEW QUESTION # 135

This file has been manually created on a universal forwarder

□ A new Splunk admin comes in and connects the universal forwarders to a deployment server and deploys the same app with a new
□ Which file is now monitored?

- A. /var/log/messages
- B. none of the above
- C. /var/log/maillog and /var/log/messages
- D. /var/log/maillog

Answer: D

NEW QUESTION # 136

Which of the following indexes come pre-configured with Splunk Enterprise? (select all that apply)

- A. _external
- B. _thefishbucket
- C. _license
- D. _internal

Answer: B,D

Explanation:

<https://docs.splunk.com/Documentation/Splunk/8.0.5/Indexer/Howindexingworks>

NEW QUESTION # 137

What is the order of precedence (from lowest # highest) within serverclass.conf in which attributes will be expressed?

- A. [global] # [serverClass:<name>] # [serverClass:<name>:client:<client.name>:user:<username>]
- B. [global] # [serverClass:<name>] # [app:<appname>]
- C. [global] # [serverClass:<name>] # [serverClass:<name>:app:<appname>]
- D. [global] # [serverClass:<name>] # [serverClass:<name>:client:<client.name>]

Answer: C

Explanation:

The serverclass.conf file controls how deployment apps and configurations are distributed from the Deployment Server to its Deployment Clients. Within this configuration, attribute values can be defined at multiple levels, and Splunk applies them based on a defined order of precedence - from general to most specific.

The correct order of evaluation (lowest to highest precedence) is:

* [global] - applies to all server classes and clients unless overridden.

* [serverClass:<name>] - applies to all clients in that specific server class.

* [serverClass:<name>:app:<appname>] - applies only to a specific app within that server class and overrides previous settings.

This means that values set in the [serverClass:<name>:app:<appname>] stanza take priority over those in

[serverClass:<name>], which in turn override values in [global].

Example (from serverclass.conf):

```
[global]
```

```
whitelist.0 = *
```

```
[serverClass:web_servers]
whitelist.0 = web01*
blacklist.0 = test*
[serverClass:web_servers:app:web_monitoring]
restartSplunkWeb = true
```

Here, restartSplunkWeb = true in the app stanza overrides any inherited setting from the global or class level.

Reference (Splunk Documentation):

- * Splunk Enterprise Admin Manual # Deploy configurations using deployment server
- * serverclass.conf.spec and example # "Precedence of attributes: global < serverClass:<name> < serverClass:<name>:app:<appname>"
- * Splunk Docs: "How the deployment server works"

NEW QUESTION # 138

Which default Splunk role could be assigned to provide users with the following capabilities?

Create saved searches

Edit shared objects and alerts

Not allowed to create custom roles

- A. splunk-system-role
- B. user
- C. power
- D. admin

Answer: C

Explanation:

Reference:<https://docs.splunk.com/Documentation/Splunk/8.2.3/Admin/Aboutusersandroles> The power role is a default Splunk role that grants users the ability to create saved searches, edit shared objects and alerts, and access advanced search commands.

However, the power role does not allow users to create custom roles, which is a privilege reserved for the admin role. Therefore, option B is the correct answer. References: Splunk Enterprise Certified Admin | Splunk, [About configuring role-based user access - Splunk Documentation]

NEW QUESTION # 139

Which of the following are available input methods when adding a file input in Splunk Web? (Choose all that apply.)

- A. Monitor interval.
- B. Continuously monitor.
- C. On-demand monitor.
- D. Index once.

Answer: B,D

Explanation:

<https://docs.splunk.com/Documentation/Splunk/8.2.2/Data/Howdoyouwanttoadddata> The fastest way to add data to your Splunk Cloud instance or Splunk Enterprise deployment is to use Splunk Web. After you access the Add Data page, choose one of three options for getting data into your Splunk platform deployment with Splunk Web: (1) Upload, (2) Monitor, (3) Forward The Upload option lets you upload a file or archive of files for indexing. When you choose Upload option, Splunk Web opens the upload process page. Monitor. For Splunk Enterprise installations, the Monitor option lets you monitor one or more files, directories, network streams, scripts, Event Logs (on Windows hosts only), performance metrics, or any other type of machine data that the Splunk Enterprise instance has access to.

NEW QUESTION # 140

.....

There is no need to worry about failure when you already have the most probable Splunk Enterprise Certified Admin (SPLK-1003) questions in the Cert2Pass PDF document. All you need is to stay positive, put in your best efforts, and be confident while appearing for the Splunk SPLK-1003 Exam. Laptops, smartphones, and tablets support the PDF format.

SPLK-1003 New Cram Materials: https://www.getcertkey.com/SPLK-1003_braindumps.html

- [illegible]

BTW, DOWNLOAD part of Getcertkey SPLK-1003 dumps from Cloud Storage: <https://drive.google.com/open?id=1lhbbRsvBLEzIPX1mfPZtd2Sfcus9WS2>