

# New SPLK-2002 Exam Testking | Latest SPLK-2002 Exam Preparation



BTW, DOWNLOAD part of PracticeVCE SPLK-2002 dumps from Cloud Storage: [https://drive.google.com/open?id=1MDPEJebmPAzlgfvZGD5qiMmOBUEPG\\_ly](https://drive.google.com/open?id=1MDPEJebmPAzlgfvZGD5qiMmOBUEPG_ly)

Do you know why you feel pressured to work? That is because your own ability and experience are temporarily unable to adapt to current job requirements. To buy our SPLK-2002 practice engine at this time is to upgrade your skills and experience to the current requirements in order to have the opportunity to make the next breakthrough. And our SPLK-2002 Exam Braindumps are good to help you in developing your knowledge and skills. Besides, our SPLK-2002 study guide will reward you with the certification.

We know that tenet from the bottom of our heart, so all parts of service are made due to your interests. You are entitled to have full money back if you fail the exam even after getting our SPLK-2002 test prep. Our staff will help you with genial attitude. We esteem your variant choices so all these versions of SPLK-2002 Study Materials are made for your individual preference and inclination.

>> New SPLK-2002 Exam Testking <<

## PracticeVCE's SPLK-2002 Dumps Questions With 365 Days Free Updates

With the help of SPLK-2002 guide questions, you can conduct targeted review on the topics which to be tested before the exam, and then you no longer have to worry about the problems that you may encounter a question that you are not familiar with during the exam. With SPLK-2002 Learning Materials, you will not need to purchase any other review materials. Please be assured that with the help of SPLK-2002 learning materials, you will be able to successfully pass the exam.

## Splunk Enterprise Certified Architect Sample Questions (Q117-Q122):

### NEW QUESTION # 117

What log file would you search to verify if you suspect there is a problem interpreting a regular expression in a monitor stanza?

- A. btool.log
- B. metrics.log
- C. tailing\_processor.log
- D. splunkd.log

**Answer: D**

Explanation:

Explanation/Reference: <https://answers.splunk.com/answers/479312/how-to-edit-inputsconf-to-monitor-multiple-files-w-1.html>

### NEW QUESTION # 118

Which search head cluster component is responsible for pushing knowledge bundles to search peers, replicating configuration changes to search head cluster members, and scheduling jobs across the search head cluster?

- A. Deployer
- **B. Captain**
- C. Deployment server
- D. Master

**Answer: B**

Explanation:

Explanation

The captain is the search head cluster component that is responsible for pushing knowledge bundles to search peers, replicating configuration changes to search head cluster members, and scheduling jobs across the search head cluster. The captain is elected from among the search head cluster members and performs these tasks in addition to serving search requests. The master is the indexer cluster component that is responsible for managing the replication and availability of data across the peer nodes. The deployer is the standalone instance that is responsible for distributing apps and other configurations to the search head cluster members. The deployment server is the instance that is responsible for distributing apps and other configurations to the deployment clients, such as forwarders

### NEW QUESTION # 119

Several critical searches that were functioning correctly yesterday are not finding a lookup table today. Which log file would be the best place to start troubleshooting?

- A. health.log
- B. btool.log
- **C. web\_access.log**
- D. configuration\_change.log

**Answer: C**

Explanation:

A lookup table is a file that contains a list of values that can be used to enrich or modify the data during search time<sup>1</sup>. Lookup tables can be stored in CSV files or in the KV Store<sup>1</sup>. Troubleshooting lookup tables involves identifying and resolving issues that prevent the lookup tables from being accessed, updated, or applied correctly by the Splunk searches. Some of the tools and methods that can help with troubleshooting lookup tables are:

\* web\_access.log: This is a file that contains information about the HTTP requests and responses that occur between the Splunk web server and the clients<sup>2</sup>. This file can help troubleshoot issues related to lookup table permissions, availability, and errors, such as 404 Not Found, 403 Forbidden, or 500 Internal Server Error<sup>3</sup>.

\* btool output: This is a command-line tool that displays the effective configuration settings for a given Splunk component, such as inputs, outputs, indexes, props, and so on<sup>5</sup>. This tool can help troubleshoot issues related to lookup table definitions, locations, and precedence, as well as identify the source of a configuration setting<sup>6</sup>.

\* search.log: This is a file that contains detailed information about the execution of a search, such as the search pipeline, the search commands, the search results, the search errors, and the search performance.

This file can help troubleshoot issues related to lookup table commands, arguments, fields, and outputs, such as lookup, inputlookup, outputlookup, lookup\_editor, and so on.

Option B is the correct answer because web\_access.log is the best place to start troubleshooting lookup table issues, as it can provide the most relevant and immediate information about the lookup table access and status.

Option A is incorrect because btool output is not a log file, but a command-line tool. Option C is incorrect because health.log is a file that contains information about the health of the Splunk components, such as the indexer cluster, the search head cluster, the license master, and the deployment server. This file can help troubleshoot issues related to Splunk deployment health, but not necessarily related to lookup tables. Option D is incorrect because configuration\_change.log is a file that contains information about the changes made to the Splunk configuration files, such as the user, the time, the file, and the action. This file can help troubleshoot issues related to Splunk configuration changes, but not necessarily related to lookup tables.

References:

1: About lookups - Splunk Documentation 2: web\_access.log - Splunk Documentation 3: Troubleshoot lookups to the Splunk Enterprise KV Store 4: Troubleshoot lookups in Splunk Enterprise Security - Splunk Documentation 5: Use btool to troubleshoot configurations - Splunk Documentation 6: Troubleshoot configuration issues - Splunk Documentation : Use the search.log file - Splunk Documentation : Troubleshoot search-time field extraction - Splunk Documentation : [Troubleshoot lookups - Splunk

Documentation] :

[health.log - Splunk Documentation] : [configuration\_change.log - Splunk Documentation]

### NEW QUESTION # 120

(What command will decommission a search peer from an indexer cluster?)

- A. splunk disablepeer --enforce-counts
- B. splunk remove cluster-peers -enforce-counts
- C. splunk offline -enforce-counts
- D. splunk decommission -enforce-counts

**Answer: C**

Explanation:

The splunk offline --enforce-counts command is the official and documented method used to gracefully decommission a search peer (indexer) from an indexer cluster in Splunk Enterprise. This command ensures that all replication and search factors are maintained before the peer is removed.

When executed, Splunk initiates a controlled shutdown process for the peer node. The Cluster Manager verifies that sufficient replicated copies of all bucket data exist across the remaining peers according to the configured replication\_factor (RF) and search\_factor (SF). The --enforce-counts flag specifically enforces that replication and search counts remain intact before the peer fully detaches from the cluster, ensuring no data loss or availability gap.

The sequence typically includes:

- \* Validating cluster state and replication health.
- \* Rolling off the peer's data responsibilities to other peers.
- \* Removing the peer from the active cluster membership list once replication is complete.

Other options like disablepeer, decommission, or remove cluster-peers are not valid Splunk commands.

Therefore, the correct documented method is to use:

```
splunk offline --enforce-counts
```

References (Splunk Enterprise Documentation):

- \* Indexer Clustering: Decommissioning a Peer Node
- \* Managing Peer Nodes and Maintaining Data Availability
- \* Splunk CLI Command Reference - splunk offline
- \* Cluster Manager and Peer Maintenance Procedures

### NEW QUESTION # 121

Which of the following are client filters available in serverclass.conf? (Select all that apply.)

- A. DNS name.
- B. Splunk server role.
- C. IP address.
- D. Platform (machine type).

**Answer: A,C**

### NEW QUESTION # 122

.....

Our company concentrates on relieving your pressure of preparing the SPLK-2002 exam. Getting the certificate equals to embrace a promising future and good career development. Perhaps you have heard about our SPLK-2002 exam question from your friends or news. Why not has a brave attempt? You will certainly benefit from your wise choice. Now our SPLK-2002 practice materials have won customers' strong support. Our sales volume is increasing every year. The great achievements benefit from our enormous input. First of all, we have done good job on researching the new version of the SPLK-2002 exam question.

**Latest SPLK-2002 Exam Preparation:** <https://www.practicevce.com/Splunk/SPLK-2002-practice-exam-dumps.html>

You just need to use spare time to practice the Splunk SPLK-2002 dumps questions and remember the key knowledge of SPLK-2002 dumps torrent, Splunk New SPLK-2002 Exam Testking Our main goal is customer satisfaction, Some people have to obtain the Latest SPLK-2002 Exam Preparation - Splunk Enterprise Certified Architect certification due to the requirement of the

company, Our SPLK-2002 practice materials can provide the knowledge you need to know how to pass the Splunk Enterprise Certified Architect practice exam successfully.

There will be several proctors walking around the room while SPLK-2002 you are taking the test, That way, we can let the library type manage the storage for the elements themselves.

You just need to use spare time to practice the Splunk SPLK-2002 Dumps Questions and remember the key knowledge of SPLK-2002 dumps torrent, Our main goal is customer satisfaction.

## **Trusted New SPLK-2002 Exam Testking & Useful Splunk Certification Training - Trustworthy Splunk Splunk Enterprise Certified Architect**

Some people have to obtain the Splunk Enterprise Certified Architect certification due to the requirement of the company, Our SPLK-2002 practice materials can provide the knowledge you need to know how to pass the Splunk Enterprise Certified Architect practice exam successfully.

Passing the SPLK-2002 practice test is absolutely an indispensable part to realize your dreams like that.

- Free PDF Quiz 2026 Latest Splunk New SPLK-2002 Exam Testking  Open **【 www.testkingpass.com 】** and search for ▷ SPLK-2002 ◁ to download exam materials for free  SPLK-2002 Best Vce
- Valid SPLK-2002 Test Review  SPLK-2002 Top Questions  ExamDumps SPLK-2002 Pdf  Search on ➡ www.pdfvce.com  for ✨ SPLK-2002  ✨  to obtain exam materials for free download  Exam Dumps SPLK-2002 Pdf
- Free PDF Quiz 2026 Pass-Sure SPLK-2002: New Splunk Enterprise Certified Architect Exam Testking  Search on 「 www.pdfdumps.com 」 for ▷ SPLK-2002 ◁ to obtain exam materials for free download  ExamDumps SPLK-2002 Pdf
- SPLK-2002 Valid Test Topics  Valid Dumps SPLK-2002 Book  SPLK-2002 Reliable Test Blueprint  Search for ➡ SPLK-2002  and easily obtain a free download on ➡ www.pdfvce.com   SPLK-2002 Valid Test Topics
- Reliable Study SPLK-2002 Questions  ExamDumps SPLK-2002 Pdf  SPLK-2002 Valid Exam Papers  Open ➡ www.easy4engine.com  enter  SPLK-2002  and obtain a free download  Exam Dumps SPLK-2002 Pdf
- New New SPLK-2002 Exam Testking | Valid SPLK-2002: Splunk Enterprise Certified Architect 100% Pass  Copy URL ▷ www.pdfvce.com ◁ open and search for { SPLK-2002 } to download for free  SPLK-2002 Valid Exam Papers
- SPLK-2002 Valid Test Topics  SPLK-2002 Top Questions  Study Guide SPLK-2002 Pdf ✨ Open website  www.prep4away.com  and search for ( SPLK-2002 ) for free download  SPLK-2002 Best Vce
- Valid SPLK-2002 Practice Materials  Valid Dumps SPLK-2002 Book  SPLK-2002 Reliable Braindumps Files  Copy URL 《 www.pdfvce.com 》 open and search for [ SPLK-2002 ] to download for free  SPLK-2002 Top Questions
- High Pass-Rate New SPLK-2002 Exam Testking - Easy and Guaranteed SPLK-2002 Exam Success  Go to website ✓ www.troytecdumps.com  ✓  open and search for ➡ SPLK-2002  to download for free  SPLK-2002 Best Vce
- Reliable SPLK-2002 Test Prep  Study Guide SPLK-2002 Pdf  SPLK-2002 Valid Exam Papers  Search for ➡ SPLK-2002  and download it for free immediately on { www.pdfvce.com }  Exam Dumps SPLK-2002 Pdf
- New New SPLK-2002 Exam Testking | Valid SPLK-2002: Splunk Enterprise Certified Architect 100% Pass ↖ Go to website ➡ www.prepawaypdf.com  open and search for ✓ SPLK-2002  ✓  to download for free  Valid SPLK-2002 Practice Materials
- pennyonfs374485.governor-wiki.com, explorebookmarks.com, sairauxzq235584.losblogos.com, deweyrqb078834.verybigblog.com, www.stes.tyc.edu.tw, deweypphd538421.blogaritma.com, gregoryniwn151712.blogdeazar.com, www.stes.tyc.edu.tw, www.stes.tyc.edu.tw, safagmeb972951.liberty-blog.com, Disposable vapes

P.S. Free 2026 Splunk SPLK-2002 dumps are available on Google Drive shared by PracticeVCE: [https://drive.google.com/open?id=1MDPEJebmPAzlgfZGD5qiMmOBUEPG\\_ly](https://drive.google.com/open?id=1MDPEJebmPAzlgfZGD5qiMmOBUEPG_ly)