

SPLK-2002 Certification Dump | SPLK-2002 Valid Exam Bootcamp



BTW, DOWNLOAD part of DumpsTorrent SPLK-2002 dumps from Cloud Storage: https://drive.google.com/open?id=1hnuUqcDxhu0-BV2BR3n9PEc_8dFinOra

According to the statistic about candidates, we find that some of them take part in the Splunk exam for the first time. Considering the inexperience of most candidates, we provide some free trail for our customers to have a basic knowledge of the SPLK-2002 exam guide and get the hang of how to achieve the SPLK-2002 exam certification in their first attempt. You can download a small part of PDF demo, which is in a form of questions and answers relevant to your coming SPLK-2002 Exam; and then you may have a decision about whether you are content with it. In fact, there are no absolutely right SPLK-2002 exam questions for you; there is just a suitable learning tool for your practices. Therefore, for your convenience and your future using experience, we sincere suggest you to have a download to before payment.

Once our professionals find the relevant knowledge on the SPLK-2002 exam questions, then the whole research groups will pick out the knowledge points according to the test syllabus. Also, they will also compile some questions about the SPLK-2002 practice materials in terms of their experience. Now, we have successfully summarized all knowledge points in line with the SPLK-2002 outline. And meanwhile, we keep a close eye on the changes of the exam to make sure what you buy are the latest and valid.

>> SPLK-2002 Certification Dump <<

Verified SPLK-2002 Certification Dump & Leader in Qualification Exams & Reliable SPLK-2002: Splunk Enterprise Certified Architect

Are you planning to crack the Splunk Splunk Enterprise Certified Architect SPLK-2002 certification test in a short time and don't know how to prepare for it? DumpsTorrent has updated SPLK-2002 Dumps questions for the applicants who want to prepare for the Splunk SPLK-2002 Certification test successfully within a few days. This study material is available in three different formats that you can trust to crack the Splunk SPLK-2002 certification test with ease.

Splunk Enterprise Certified Architect Sample Questions (Q129-Q134):

NEW QUESTION # 129

At which default interval does metrics.log generate a periodic report regarding license utilization?

- A. 30 seconds
- B. 10 seconds
- C. 300 seconds
- **D. 60 seconds**

Answer: D

Explanation:

The default interval at which metrics.log generates a periodic report regarding license utilization is 60 seconds. This report contains information about the license usage and quota for each Splunk instance, as well as the license pool and stack. The report is generated every 60 seconds by default, but this interval can be changed by modifying the license_usage stanza in the metrics.conf file. The other intervals (10 seconds, 30 seconds, and 300 seconds) are not the default values, but they can be set by the administrator if needed. For more information, see About metrics.log and Configure metrics.log in the Splunk documentation.

NEW QUESTION # 130

Because Splunk indexing is read/write intensive, it is important to select the appropriate disk storage solution for each deployment. Which of the following statements is accurate about disk storage?

- A. High performance SAN should never be used.
- **B. The recommended RAID setup is RAID 10 (1 + 0).**
- C. Enable NFS for storing hot and warm buckets.
- D. Virtualized environments are usually preferred over bare metal for Splunk indexers.

Answer: B

Explanation:

Explanation/Reference: <https://www.splunk.com/pdfs/technical-briefs/splunk-deploying-vmware-tech-brief.pdf>

NEW QUESTION # 131

(On which Splunk components does the Splunk App for Enterprise Security place the most load?)

- A. Cluster Managers
- B. Heavy Forwarders
- C. Indexers
- **D. Search Heads**

Answer: D

Explanation:

According to Splunk's Enterprise Security (ES) Installation and Sizing Guide, the majority of processing and computational load generated by the Splunk App for Enterprise Security is concentrated on the Search Head (s).

This is because Splunk ES is built around a search-driven correlation model - it continuously runs scheduled correlation searches, data model accelerations, and notables generation jobs. These operations rely on the search head tier's CPU, memory, and I/O resources rather than on indexers. ES also performs extensive data model summarization, CIM normalization, and real-time alerting, all of which are search-intensive operations.

While indexers handle data ingestion and indexing, they are not heavily affected by ES beyond normal search request processing. The Cluster Manager only coordinates replication and plays no role in search execution, and Heavy Forwarders serve as data collection or parsing points with minimal analytical load.

Splunk officially recommends deploying ES on a dedicated Search Head Cluster (SHC) to isolate its high CPU and memory demands from other workloads. For large-scale environments, horizontal scaling via SHC ensures consistent performance and stability.

References (Splunk Enterprise Documentation):

- * Splunk Enterprise Security Installation and Configuration Guide
- * Search Head Sizing for Splunk Enterprise Security
- * Enterprise Security Overview - Workload Distribution and Performance Impact
- * Splunk Architecture and Capacity Planning for ES Deployments

NEW QUESTION # 132

Which of the following is a best practice to maximize indexing performance?

- A. Not use pre-trained source types.
- B. Use the Splunk default settings.
- C. Use automatic source typing.
- D. **Minimize configuration generality.**

Answer: D

Explanation:

A best practice to maximize indexing performance is to minimize configuration generality. Configuration generality refers to the use of generic or default settings for data inputs, such as source type, host, index, and timestamp. Minimizing configuration generality means using specific and accurate settings for each data input, which can reduce the processing overhead and improve the indexing throughput. Using automatic source typing, using the Splunk default settings, and not using pre-trained source types are examples of configuration generality, which can negatively affect the indexing performance

NEW QUESTION # 133

Which of the following is unsupported in a production environment?

- A. **Indexers in an indexer cluster can run on virtual machines.**
- B. Search heads in a Search Head Cluster can run on virtual machines.
- C. Search Head Cluster Deployer can run on the Monitoring Console instance in smaller environments.
- D. **Cluster Manager can run on the Monitoring Console instance in smaller environments.**

Answer: A,D

Explanation:

Comprehensive and Detailed Explanation (From Splunk Enterprise Documentation)Splunk Enterprise documentation clarifies that none of the listed configurations are prohibited in production. Splunk allows the Cluster Manager to be colocated with the Monitoring Console in small deployments because both are management-plane functions and do not handle ingestion or search traffic. The documentation also states that the Search Head Cluster Deployer is not a runtime component and has minimal performance requirements, so it may be colocated with the Monitoring Console or Licensing Master when hardware resources permit.

Splunk also supports virtual machines for both search heads and indexers, provided they are deployed with dedicated CPU, storage throughput, and predictable performance. Splunk's official hardware guidance specifies that while bare metal often yields higher performance, virtualized deployments are fully supported in production as long as sizing principles are met.

Because Splunk explicitly supports all four configurations under proper sizing and best-practice guidelines, there is no correct selection for "unsupported." The question is outdated relative to current Splunk Enterprise recommendations.

References:Splunk Validated Architectures (Component Roles and Colocation Guidance); Splunk Search Head Clustering Manual; Splunk Indexer Clustering Manual; Splunk Hardware and Performance Recommendations.

NEW QUESTION # 134

.....

You can write down your doubts or any other question of our Splunk Enterprise Certified Architect test questions. We warmly welcome all your questions. Our online workers are responsible for solving all your problems with twenty four hours service. You still can enjoy our considerate service after you have purchased our SPLK-2002 test guide. If you don't know how to install the study materials, our professional experts can offer you remote installation guidance. Also, we will offer you help in the process of using our SPLK-2002 Exam Questions. Also, if you have better suggestions to utilize our study materials, we will be glad to take it seriously.

SPLK-2002 Valid Exam Bootcamp: <https://www.dumpstorrent.com/SPLK-2002-exam-dumps-torrent.html>

If you still feel difficult in preparing for your exam and passing exam, our SPLK-2002 exam materials will be helpful for you, Splunk SPLK-2002 Certification Dump Thirdly,it is convenient for studying, Safely use the questions provided by DumpsTorrent SPLK-2002 Valid Exam Bootcamp's products, Advance Your Abilities With Splunk SPLK-2002 Exam, If you think i'm exaggerating, you might as well take a look at our SPLK-2002 actual exam.

Miniaturized electronics led the way to digital SPLK-2002 computers—originally the size of refrigerators. Customizing system devices. If you still feel difficult in preparing for your exam and passing exam, our SPLK-2002 Exam Materials will be helpful for you.

SPLK-2002 Certification Dump - 100% Pass Quiz 2026 SPLK-2002: First-grade Splunk Enterprise Certified Architect Valid Exam Bootcamp

Thirdly, it is convenient for studying. Safely SPLK-2002 Certification Dump use the questions provided by DumpsTorrent's products, Advance Your Abilities With Splunk SPLK-2002 Exam. If you think i'm exaggerating, you might as well take a look at our SPLK-2002 actual exam.

2026 Latest DumpsTorrent SPLK-2002 PDF Dumps and SPLK-2002 Exam Engine Free Share: https://drive.google.com/open?id=1hnwUqcDxhu0-BV2BR3n9PEc_8dFinOra