Quiz Splunk - SPLK-2002–Trustable Latest Test Dumps

[Feb-2023] Latest Splunk SPLK-2002 Certification Practice Test Questions [Q28-Q42]

2025 Latest PremiumVCEDump SPLK-2002 PDF Dumps and SPLK-2002 Exam Engine Free Share: https://drive.google.com/open?id=16vtpO0GBgKRKVEKWKNF-Ni36FQs_kNJw

We provide 1 year of free updates. In conclusion, PremiumVCEDump guarantees that if you use the product, you will pass the SPLK-2002 exam on your first try. Its primary goal is to save students time and money, not just conduct a business transaction. Candidates can take advantage of the free trials to evaluate the quality and standard of the SPLK-2002 Dumps before making a purchase. With the right SPLK-2002 study material and support team passing the examination at first attempt is an achievable goal.

To prepare for the SPLK-2002 Certification Exam, candidates should review the exam objectives and study the Splunk documentation. Splunk also offers training courses that cover the exam content in depth. Candidates can also participate in Splunk user groups and online communities to connect with other Splunk professionals and learn from their experiences.

>> SPLK-2002 Latest Test Dumps <<

100% Pass Quiz Splunk - SPLK-2002 - Unparalleled Splunk Enterprise Certified Architect Latest Test Dumps

Improve your professional ability with our SPLK-2002 certification. Getting qualified by the Splunk certification will position you for better job opportunities and higher salary. Now, let's start your preparation with SPLK-2002 training material. The SPLK-2002 practice pdf offered by PremiumVCEDump latest pdf is the latest and valid study material which suitable for all of you. The SPLK-2002 free demo is especially for you to free download for try before you buy. You can get a lot from the SPLK-2002 simulate exam dumps and get your SPLK-2002 certification easily.

Splunk Enterprise Certified Architect Sample Questions (Q17-Q22):

NEW QUESTION # 17
Which of the following statements about integrating with third-party systems is true? (Select all that apply.)

- A. You can use Splunk alerts to provision actions on a third-party system.
- B. Splunk can search data in the Hadoop File System (HDFS).
- C. A Hadoop application can search data in Splunk.
- D. You can forward data from Splunk forwarder to a third-party system without indexing it first.

Answer: A,D

Explanation:
Explanation
The following statements about integrating with third-party systems are true: You can use Splunk alerts to provision actions on a third-party system, and you can forward data from Splunk forwarder to a third-party system without indexing it first. Splunk alerts

are triggered events that can execute custom actions, such as sending an email, running a script, or calling a webhook. Splunk alerts can be used to integrate with third-party systems, such as ticketing systems, notification services, or automation platforms. For example, you can use Splunk alerts to create a ticket in ServiceNow, send a message to Slack, or trigger a workflow in Ansible. Splunk forwarders are Splunk instances that collect and forward data to other Splunk instances, such as indexers or heavy forwarders. Splunk forwarders can also forward data to third-party systems, such as Hadoop, Kafka, or AWS Kinesis, without indexing it first. This can be useful for sending data to other data processing or storage systems, or for integrating with other analytics or monitoring tools. A Hadoop application cannot search data in Splunk, because Splunk does not provide a native interface for Hadoop applications to access Splunk data. Splunk can search data in the Hadoop File System (HDFS), but only by using the Hadoop Connect app, which is a Splunk app that enables Splunk to index and search data stored in HDFS

NEW QUESTION # 18

When planning a search head cluster, which of the following is true?

- A. All search heads must use the same operating system.
- B. All search heads must be members of the cluster (no standalone search heads).
- C. All indexers must belong to the underlying indexer cluster (no standalone indexers).
- D. The search head captain must be assigned to the largest search head in the cluster.

Answer: C

Explanation:
Explanation
When planning a search head cluster, the following statement is true: All indexers must belong to the underlying indexer cluster (no standalone indexers). A search head cluster is a group of search heads that share configurations, apps, and search jobs. A search head cluster requires an indexer cluster as its data source, meaning that all indexers that provide data to the search head cluster must be members of the same indexer cluster. Standalone indexers, or indexers that are not part of an indexer cluster, cannot be used as data sources for a search head cluster. All search heads do not have to use the same operating system, as long as they are compatible with the Splunk version and the indexer cluster. All search heads do not have to be members of the cluster, as standalone search heads can also search the indexer cluster, but they will not have the benefits of configuration replication and load balancing. The search head captain does not have to be assigned to the largest search head in the cluster, as the captain is dynamically elected from among the cluster members based on various criteria, such as CPU load, network latency, and search load.

NEW QUESTION # 19

(Which of the following is a minimum search head specification for a distributed Splunk environment?)

- A. An x86 32-bit chip architecture.
- B. 128 GB RAM.
- C. A 1Gb Ethernet NIC, optional 2nd NIC for a management network.
- D. Two physical CPU cores, or four vCPU at 2GHz or greater speed per core.

Answer: D

Explanation:
According to the Splunk Enterprise Capacity Planning and Hardware Sizing Guidelines, a distributed Splunk environment's minimum search head specification must ensure that the system can efficiently manage search parsing, ad-hoc query execution, and knowledge object replication. Splunk officially recommends using a 64- bit x86 architecture system with a minimum of two physical CPU cores (or four vCPUs) running at 2 GHz or higher per core for acceptable performance.
Search heads are CPU-intensive components, primarily constrained by processor speed and the number of concurrent searches they must handle. Memory and disk space should scale with user concurrency and search load, but CPU capability remains the baseline requirement. While 128 GB RAM (Option C) is suitable for high-demand or Enterprise Security (ES) deployments, it exceeds the minimum hardware specification for general distributed search environments.
Splunk no longer supports 32-bit architectures (Option B). While a 1Gb Ethernet NIC (Option A) is common, it is not part of the minimum computational specification required by Splunk for search heads. The critical specification is processor capability - two physical cores or equivalent.
References (Splunk Enterprise Documentation):
* Splunk Enterprise Capacity Planning Manual - Hardware and Performance Guidelines
* Search Head Sizing and System Requirements
* Distributed Deployment Manual - Recommended System Specifications
* Splunk Hardware and Performance Tuning Guide

NEW QUESTION # 20
Which index-time props.conf attributes impact indexing performance? (Select all that apply.)

- A. REPORT
- B. LINE_BREAKER
- C. ANNOTATE_PUNCT
- D. SHOULD_LINEMERGE

Answer: B,D

Explanation:
Explanation
The index-time props.conf attributes that impact indexing performance are LINE_BREAKER and SHOULD_LINEMERGE. These attributes determine how Splunk breaks the incoming data into events and whether it merges multiple events into one. These operations can affect the indexing speed and the disk space consumption. The REPORT attribute does not impact indexing performance, as it is used to apply transforms at search time. The ANNOTATE_PUNCT attribute does not impact indexing performance, as it is used to add punctuation metadata to events at search time. For more information, see [About props.conf and transforms.conf] in the Splunk documentation.

NEW QUESTION # 21
A new Splunk customer is using syslog to collect data from their network devices on port 514. What is the best practice for ingesting this data into Splunk?

- A. Use a Splunk forwarder to collect the input on port 514 and forward the data.
- B. Configure syslog to send the data to multiple Splunk indexers.
- C. Configure syslog to write logs and use a Splunk forwarder to collect the logs.
- D. Use a Splunk indexer to collect a network input on port 514 directly.

Answer: C

Explanation:
Explanation
The best practice for ingesting syslog data from network devices on port 514 into Splunk is to configure syslog to write logs and use a Splunk forwarder to collect the logs. This practice will ensure that the data is reliably collected and forwarded to Splunk, without losing any data or overloading the Splunk indexer. Configuring syslog to send the data to multiple Splunk indexers will not guarantee data reliability, as syslog is a UDP protocol that does not provide acknowledgment or delivery confirmation. Using a Splunk indexer to collect a network input on port 514 directly will not provide data reliability or load balancing, as the indexer may not be able to handle the incoming data volume or distribute it to other indexers. Using a Splunk forwarder to collect the input on port 514 and forward the data will not provide data reliability, as the forwarder may not be able to receive the data from syslog or buffer it in case of network issues. For more information, see [Get data from TCP and UDP ports] and [Best practices for syslog data] in the Splunk documentation.

NEW QUESTION # 22
......

Exam SPLK-2002 tests your professional talent and expertise. This is the reason that passing this Splunk Enterprise Certified Architect certification exam has been a tough challenge for professionals. But it is made easy now to ace it! The recently developed PremiumVCEDump's SPLK-2002 Exam Questions dumps aim at to deliver you the shortest possible route to obtaining SPLK-2002 without any chance of losing the exam.

SPLK-2002 Test Review: https://www.premiumvcedump.com/Splunk/valid-SPLK-2002-premium-vce-exam-dumps.html

- Certification SPLK-2002 Torrent □ SPLK-2002 Exams Dumps □ SPLK-2002 Reliable Exam Blueprint □ Immediately open 《 www.lead1pass.com 》 and search for □ SPLK-2002 □ to obtain a free download □Valid SPLK-2002 Test Objectives
- New Release SPLK-2002 PDF Dumps [2025] - SPLK-2002 Splunk Enterprise Certified Architect Exam Questions □ Open □ www.pdfvce.com □ enter ➡ SPLK-2002 □□□ and obtain a free download □SPLK-2002 Valid Test Pdf
- Reliable SPLK-2002 Exam Prep □ SPLK-2002 Training Questions □ SPLK-2002 Valid Test Pdf □ Simply search

for ➤ SPLK-2002 □ for free download on ➽ www.examcollectionpass.com □ □Study SPLK-2002 Center

- Enhance Your Preparation with the Splunk SPLK-2002 Online Practice Test Engine □ Open { www.pdfvce.com } and search for { SPLK-2002 } to download exam materials for free □SPLK-2002 Hot Questions
- Splunk SPLK-2002 Latest Test Dumps: Splunk Enterprise Certified Architect - www.dumps4pdf.com Products Prepare for your Exam in Short Time □ Search for ✔ SPLK-2002 □✔□ and obtain a free download on ▹ www.dumps4pdf.com ◃ □SPLK-2002 Hot Questions
- Efficient SPLK-2002 Latest Test Dumps, SPLK-2002 Test Review □ Easily obtain free download of ▹ SPLK-2002 ◃ by searching on ➠ www.pdfvce.com □ □SPLK-2002 Reliable Exam Blueprint
- SPLK-2002 Exams Dumps □ SPLK-2002 Valid Braindumps Book □ Study SPLK-2002 Center □ Search on ➽ www.actual4labs.com □ for ➠ SPLK-2002 □ to obtain exam materials for free download □SPLK-2002 Training Questions
- SPLK-2002 Latest Test Dumps - Effective SPLK-2002 Test Review and Valid Test Splunk Enterprise Certified Architect Score Report Ⓜ Open website □ www.pdfvce.com □ and search for ➽ SPLK-2002 □ for free download □SPLK-2002 Valid Braindumps Book
- SPLK-2002 Latest Test Dumps - Effective SPLK-2002 Test Review and Valid Test Splunk Enterprise Certified Architect Score Report □ Download 「 SPLK-2002 」 for free by simply entering 「 www.exams4collection.com 」 website □ □SPLK-2002 Valid Test Pdf
- SPLK-2002 Latest Test Dumps - Effective SPLK-2002 Test Review and Valid Test Splunk Enterprise Certified Architect Score Report □ Search for ➽ SPLK-2002 □ and download it for free on ➠ www.pdfvce.com □ website □Valid SPLK-2002 Test Cram
- SPLK-2002 Exams Dumps ↘ SPLK-2002 Cert Guide □ SPLK-2002 Training Questions □ Open ⇛ www.free4dump.com ⇚ and search for ⇛ SPLK-2002 ⇚ to download exam materials for free □SPLK-2002 Valid Braindumps Book
- bbs.sdhuifa.com, www.stes.tyc.edu.tw, lms.ait.edu.za, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, www.stes.tyc.edu.tw, www.stes.tyc.edu.tw, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, nualkale.pointblog.net, www.stes.tyc.edu.tw, e.871v.com, Disposable vapes

BONUS!!! Download part of PremiumVCEDump SPLK-2002 dumps for free: https://drive.google.com/open?id=16vtpO0GBgKRKVEKWKNF-Ni36FQs_kNJw