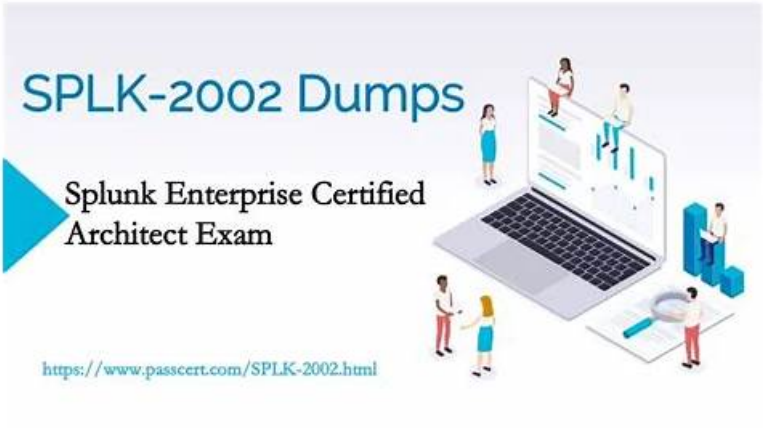
SPLK-2002시험대비공부하기, SPLK-2002인기자격증 시험대비공부자료



BONUS!!! Fast2test SPLK-2002 시험 문제집 전체 버전을 무료로 다운로드하세요: https://drive.google.com/open?id=1G36w2oYCyQb0ozMYrKsvTswqI6Zu6cFw

만약 시험만 응시하고 싶으시다면 우리의 최신Splunk SPLK-2002자료로 시험 패스하실 수 있습니다. Fast2test 의 학습가이드에는Splunk SPLK-2002인증시험의 예상문제, 시험문제와 답 임으로 100% 시험을 패스할 수 있습니다.우리의Splunk SPLK-2002시험자료로 충분한 시험준비하시는것이 좋을것 같습니다. 그리고 우리는 일년무료 업데이트를 제공합니다.

Splunk SPLK-2002인증덤프는 실제 SPLK-2002시험의 가장 최근 시험의 기출문제를 기준으로 하여 만들어진 최고품질을 자랑하는 최고적중율의 시험대비자료입니다. 저희 SPLK-2002덤프로 SPLK-2002시험에 도전해보지 않으실래요? SPLK-2002시험에서 불합격 받을시 덤프비용은 환불해드리기에 부담없이 구매하셔도 됩니다.환불의 유일한 기준은 불합격 성적표이고 환불유효기간은 구매일로부터 60일까지입니다.

>> SPLK-2002시험대비 공부하기 <<

최신버전 SPLK-2002시험대비 공부하기 완벽한 덤프문제

Fast2test의Splunk인증 SPLK-2002시험덤프 공부가이드는 시장에서 가장 최신버전이자 최고의 품질을 지닌 시험공부자료입니다.IT업계에 종사중이라면 IT자격증취득을 승진이나 연봉협상의 수단으로 간주하고 자격증취득을 공을 들여야 합니다.회사다니면서 공부까지 하려면 몸이 힘들어 스트레스가 많이 쌓인다는것을 헤아려주는Fast2test가 IT인증자격증에 도전하는데 성공하도록Splunk인증 SPLK-2002시험대비덤프를 제공해드립니다.

SPLK-2002 시험은 복잡한 Splunk Enterprise 배포를 설계하고 구현하는 능력을 평가하는 포괄적이고 실전적인 시험입니다. 이 시험은 Splunk Enterprise 아키텍처, 배포 계획, 데이터 입력 및 인덱싱, 검색 및 분석, 지식 객체 및 시스템 관리와 같은 다양한 주제를 다룹니다. 후보자들은 조직의 요구 사항을 충족시키는 Splunk Enterprise 시스템을 설계하고 구현하는 데 전문성을 증명해야 합니다. 성공적으로 SPLK-2002 시험을 마치면 IT 산업에서 귀중한 자격증으로 인정되는 Splunk Enterprise 인증 아키텍트 자격증을 받게 됩니다.

최신 Splunk Enterprise Certified Architect SPLK-2002 무료샘플문제 (Q171-Q176):

질문 # 171
Which of the following will cause the greatest reduction in disk size requirements for a cluster of N indexers running Splunk Enterprise Security?

- A. Setting the cluster replication factor to N-1.
- B. Decreasing the data model acceleration range.
- C. Increasing the number of buckets per index.
- D. Setting the cluster search factor to N-1.

정답：B

설명：
Explanation
Decreasing the data model acceleration range will reduce the disk size requirements for a cluster of indexers running Splunk Enterprise Security. Data model acceleration creates tsidx files that consume disk space on the indexers. Reducing the acceleration range will limit the amount of data that is accelerated and thus save disk space. Setting the cluster search factor or replication factor to N-1 will not reduce the disk size requirements, but rather increase the risk of data loss. Increasing the number of buckets per index will also increase the disk size requirements, as each bucket has a minimum size. For more information, see Data model acceleration and Bucket size in the Splunk documentation.

질문 # 172
A Splunk user successfully extracted an ip address into a field called src_ip. Their colleague cannot see that field in their search results with events known to have src_ip. Which of the following may explain the problem? (Select all that apply.)

- A. The colleague did not explicitly use the field in the search and the search was set to Fast Mode.
- B. The field was extracted as a private knowledge object.
- C. The events are tagged as communicate, but are missing the network tag.
- D. The Typing Queue, which does regular expression replacements, is blocked.

정답：A,B

설명：
The following may explain the problem of why a colleague cannot see the src_ip field in their search results:
The field was extracted as a private knowledge object, and the colleague did not explicitly use the field in the search and the search was set to Fast Mode. A knowledge object is a Splunk entity that applies some knowledge or intelligence to the data, such as a field extraction, a lookup, or a macro. A knowledge object can have different permissions, such as private, app, or global. A private knowledge object is only visible to the user who created it, and it cannot be shared with other users. A field extraction is a type of knowledge object that extracts fields from the raw data at index time or search time. If a field extraction is created as a private knowledge object, then only the user who created it can see the extracted field in their search results. A search mode is a setting that determines how Splunk processes and displays the search results, such as Fast, Smart, or Verbose. Fast mode is the fastest and most efficient search mode, but it also limits the number of fields and events that are displayed. Fast mode only shows the default fields, such as _time, host, source, sourcetype, and _raw, and any fields that are explicitly used in the search. If a field is not used in the search and it is not a default field, then it will not be shown in Fast mode. The events are tagged as communicate, but are missing the network tag, and the Typing Queue, which does regular expression replacements, is blocked, are not valid explanations for the problem. Tags are labels that can be applied to fields or field values to make them easier to search. Tags do not affect the visibility of fields, unless they are used as filters in the search. The Typing Queue is a component of the Splunk data pipeline that performs regular expression replacements on the data, such as replacing IP addresses with host names. The Typing Queue does not affect the field extraction process, unless it is configured to do so

질문 # 173
Which of the following can a Splunk diag contain?

- A. Search history, Splunk users and their roles, running processes, indexed data
- B. Server specs, current open connections, internal Splunk log files, index listings
- C. KV store listings, internal Splunk log files, search peer bundles listings, indexed data
- D. Splunk platform configuration details, Splunk users and their roles, current open connections, index listings

정답：B

질문 # 174
Which command will permanently decommission a peer node operating in an indexer cluster?

- A. splunk offline -f
- B. splunk stop -f
- C. splunk decommission --enforce counts
- D. splunk offline --enforce-counts

정답：D

설명：
The splunk offline --enforce-counts command will permanently decommission a peer node operating in an indexer cluster. This command will remove the peer node from the cluster and delete its data. This command should be used when the peer node is no longer needed or is being replaced by another node. The splunk stop - f command will stop the Splunk service on the peer node, but it will not decommission it from the cluster. The splunk offline -f command will take the peer node offline, but it will not delete its data or enforce the replication and search factors. The splunk decommission --enforce-counts command is not a valid Splunk command. For more information, see Remove a peer node from an indexer cluster in the Splunk documentation.

질문 # 175
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 indexer to collect a network input on port 514 directly.
- B. Configure syslog to send the data to multiple Splunk indexers.
- C. Use a Splunk forwarder to collect the input on port 514 and forward the data.
- D. Configure syslog to write logs and use a Splunk forwarder to collect the logs.

정답：D

설명：
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.

질문 # 176
.....

- SPLK-2002높은 통과율 덤프공부문제 □ SPLK-2002최고품질 덤프데모 다운 □ SPLK-2002자격증참고서 □ ➥ www.dumptop.com □을(를) 열고➽ SPLK-2002 □를 입력하고 무료 다운로드를 받으십시오SPLK-2002인증시험공부
- SPLK-2002학습자료 □ SPLK-2002인기자격증 □ SPLK-2002최고품질 덤프데모 다운 □ 무료로 쉽게 다운로드하려면「 www.itdumpskr.com 」에서➡ SPLK-2002 □□□를 검색하세요SPLK-2002인증시험공부
- SPLK-2002시험합격 □ SPLK-2002인기자격증 □ SPLK-2002시험대비 인증덤프자료 □ 《 www.exampassdump.com 》을(를) 열고“ SPLK-2002 ”를 입력하고 무료 다운로드를 받으십시오SPLK-2002높은 통과율 시험대비 공부문제
- SPLK-2002시험합격 □ SPLK-2002최고품질 덤프데모 다운 □ SPLK-2002합격보장 가능 덤프문제 □ 검색만 하면[www.itdumpskr.com]에서（ SPLK-2002 ）무료 다운로드SPLK-2002시험유효자료
- SPLK-2002합격보장 가능 덤프문제 □ SPLK-2002최신 업데이트버전 인증시험자료 □ SPLK-2002높은 통과율 시험대비 공부문제 □ ⇒ www.pass4test.net ⇐에서 검색만 하면➡ SPLK-2002 □□□를 무료로 다운로드할 수 있습니다SPLK-2002학습자료
- 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, www.stes.tyc.edu.tw, www.stes.tyc.edu.tw, 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, www.stes.tyc.edu.tw, www.stes.tyc.edu.tw, Disposable vapes

BONUS!!! Fast2test SPLK-2002 시험 문제집 전체 버전을 무료로 다운로드하세요: https://drive.google.com/open?id=1G36w2oYCyQb0ozMYrKsvTswqI6Zu6cFw