# Splunk SPLK-2002 Dumps - A Way To Prepare Quickly For Exam


DOWNLOAD the newest Real4dumps SPLK-2002 PDF dumps from Cloud Storage for free: https://drive.google.com/open?id=1LfFNwnJuF5eWTOlAMiBIMPxluWFK4ygf

A good brand is not a cheap product, but a brand that goes well beyond its users' expectations. The value of a brand is that the SPLK-2002 exam questions are more than just exam preparation tool -- it should be part of our lives, into our daily lives. Do this, therefore, our SPLK-2002 question guide has become the industry well-known brands, but even so, we have never stopped the pace of progress, we have been constantly updated the SPLK-2002 real study dumps. The most important thing is that the SPLK-2002 exam questions are continuously polished to be sold, so that users can enjoy the best service that our products bring. Our SPLK-2002 real study dumps provide users with comprehensive learning materials, so that users can keep abreast of the progress of The Times.

Splunk SPLK-2002 Certification Exam is an excellent way for professionals to demonstrate their mastery of Splunk Enterprise architecture and design. Splunk Enterprise Certified Architect certification is highly regarded by employers and is a valuable asset for individuals who are looking to advance their careers in the field of Splunk. With the increasing demand for Splunk professionals, obtaining the Splunk SPLK-2002 certification is a great way to stand out in a competitive job market.

## Splunk SPLK-2002 : Splunk Enterprise Certified Architect Exam Certified Professional salary

The average salary of a Splunk SPLK-2002 : Splunk Enterprise Certified Architect expert in:

- England - 65,632 POUND
- United State - 100,247 USD
- Europe - 60,347 EURO
- India - 15,42,327 INR

**>> New SPLK-2002 Test Objectives <<**

## Pass SPLK-2002 Guaranteed & SPLK-2002 Reliable Exam Questions

To clear the Splunk Enterprise Certified Architect SPLK-2002 exam questions in one go and not waste your time and money, follow these tips and see the result yourself. And when you know that you are ready with all the Splunk Enterprise Certified Architect SPLK-2002 Preparation, just relax, breathe and chill out. You have put your best efforts to mark your success and you shall get the best outcome out of it.

The SPLK-2002 Exam covers a wide range of topics, including data onboarding, data parsing and normalization, search optimization, clustering, monitoring and troubleshooting, and security best practices. Candidates must have a deep understanding of the Splunk platform and its various components, as well as the ability to design and implement complex Splunk deployments that meet specific business requirements.

# Splunk Enterprise Certified Architect Sample Questions (Q171-Q176):

**NEW QUESTION # 171**
To reduce the captain's work load in a search head cluster, what setting will prevent scheduled searches from running on the captain?

- A. adhoc_searchhead = true (on all members)
- B. captain_is_adhoc_searchhead = true (on the current captain)
- C. adhoc_searchhead = true (on the current captain)
- D. captain_is_adhoc_searchhead = true (on all members)

**Answer: B**

Explanation:
Explanation
To reduce the captain's work load in a search head cluster, the setting that will prevent scheduled searches from running on the captain is captain_is_adhoc_searchhead = true (on the current captain). This setting will designate the current captain as an ad hoc search head, which means that it will not run any scheduled searches, but only ad hoc searches initiated by users. This will reduce the captain's work load and improve the search head cluster performance. The adhoc_searchhead = true (on all members) setting will designate all search head cluster members as ad hoc search heads, which means that none of them will run any scheduled searches, which is not desirable. The adhoc_searchhead = true (on the current captain) setting will have no effect, as this setting is ignored by the captain. The captain_is_adhoc_searchhead = true (on all members) setting will have no effect, as this setting is only applied to the current captain. For more information, see Configure the captain as an ad hoc search head in the Splunk documentation.

**NEW QUESTION # 172**
A customer has a multisite cluster with site1 and site2 configured. They want to configure search heads in these sites to get search results only from data stored on their local sites. Which step prevents this behavior?

- A. Set site=site0 in the [general] stanza of server.conf on the search head.
- B. Configure site_search_factor = site1:2, total:3.
- C. Implement only two indexers per site.
- D. Configure site_search_factor = site1:1, total:2.

**Answer: A**

Explanation:
Comprehensive and Detailed Explanation (From Splunk Enterprise Documentation)Splunk's multisite clustering documentation describes that search affinity is controlled by the site attribute in server.conf on the search head. Splunk explicitly states that assigning site=site0 on a search head removes site affinity, causing the search head to treat all sites as equal and search remotely as needed. The documentation describes site0 as the special value that disables local-site preference and forces the system to behave like a single-site cluster.
The customer wants each site's search head to pull results only from its local site. This behavior works only if the search head's site value matches the local site name (e.g., site1 or site2). By setting it to site0, all locality restrictions are removed, which prevents the desired reduction of network traffic.
The site search factor options (B and D) affect replication and searchable copy placement on indexers, not search head behavior. The number of indexers per site (C) also does not disable search affinity. Therefore only option A disables local-only searching.
References:Splunk Indexer Clustering Manual (Multisite Search Affinity; server.conf site parameter).

**NEW QUESTION # 173**
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. Configure syslog to write logs and use a Splunk forwarder to collect the logs.
- B. Use a Splunk forwarder to collect the input on port 514 and forward the data.
- C. Use a Splunk indexer to collect a network input on port 514 directly.
- D. Configure syslog to send the data to multiple Splunk indexers.

**Answer: A**

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 # 174**
How can internal logging levels in a Splunk environment be changed to troubleshoot an issue? (select all that apply)

- A. Use Splunk Web.
- B. Edit log-local. cfg.
- C. Use the Monitoring Console (MC).
- D. Use Splunk command line.

**Answer: A,B,C,D**

Explanation:
Splunk provides various methods to change the internal logging levels in a Splunk environment to troubleshoot an issue. All of the options are valid ways to do so. Option A is correct because the Monitoring Console (MC) allows the administrator to view and modify the logging levels of various Splunk components through a graphical interface. Option B is correct because the Splunk command line provides the splunk set log-level command to change the logging levels of specific components or categories. Option C is correct because the Splunk Web provides the Settings > Server settings > Server logging page to change the logging levels of various components through a web interface. Option D is correct because the log-local.cfg file allows the administrator to manually edit the logging levels of various components by overriding the default settings in the log.cfg file123
1: https://docs.splunk.com/Documentation/Splunk/9.1.2/Troubleshooting/Enabledebuglogging 2:
https://docs.splunk.com/Documentation/Splunk/9.1.2/Admin/Serverlogging 3:
https://docs.splunk.com/Documentation/Splunk/9.1.2/Admin/Loglocalcfg

**NEW QUESTION # 175**
Which of the following is true for indexer cluster knowledge bundles?

- A. app-name/default and app-name/local are pushed without change.
- B. Only app-name/default is pushed.
- C. app-name/default and app-name/local are merged before pushing.
- D. Only app-name/local is pushed.

**Answer: C**

Explanation:
According to the Splunk documentation1, indexer cluster knowledge bundles are the configuration files that the cluster master distributes to the peer nodes as part of the cluster configuration bundle. The knowledge bundles contain the knowledge objects, such as event types, tags, lookups, and so on, that are relevant for indexing and searching the data. The cluster master creates the knowledge bundles by merging the app-name/default and app-name/local directories from the apps that reside on the master node. The cluster master then pushes the knowledge bundles to the peer nodes, where they reside under the $SPLUNK_HOME/var/run directory2. The other options are false because:
* Only app-name/local is pushed. This is false because the cluster master pushes both the app-name/default and app-name/local directories, after merging them, to the peer nodes. The app-name/local directory contains the local customizations of the app configuration, while the app-name/default directory contains the default app configuration3.
* Only app-name/default is pushed. This is false because the cluster master pushes both the app-name/default and app-name/local directories, after merging them, to the peer nodes. The app-name/default directory contains the default app configuration, while the app-name/local directory contains the local customizations of the app configuration3.
* app-name/default and app-name/local are pushed without change. This is false because the cluster
* master merges the app-name/default and app-name/local directories before pushing them to the peer nodes. This ensures that the

peer nodes have the latest and consistent configuration of the apps3.

**NEW QUESTION # 176**

.....