Splunk

SPLK-2002

Splunk Enterprise Certified Architect

Question:80

Which Splunk tool offers a health check for administrators to evaluate the health of their
Splunk deployment?

A. btool
B. DiagGen
C. SPL Clinic
D. Monitoring Console

Answer: D

Reference: https://docs.splunk.com/Documentation/Splunk/7.3.1/DMC/DMCoverview

Question: 81

In a four site indexer cluster, which configuration stores two searchable copies at the origin site, one searchable copy at site2, and a total of four searchable copies?

A. site_search_factor = origin:2, site1:2, total:4
B. site_search_factor = origin:2, site2:1, total:4
C. site_replication_factor = origin:2, site1:2, total:4
D. site_replication_factor = origin:2, site2:1, total:4

Answer: D

Reference: https://docs.splunk.com/Documentation/Splunk/7.3.2/Indexer/Sitereplicationfactor

Question: 82

A multi-site indexer cluster can be configured using which of the following? (Select all that apply.)

A. Via Splunk Web.
B. Directly edit SPLUNK_HOME/etc/system/local/server.conf
C. Run a splunk edit cluster-config command from the CLI.
D. Directly edit SPLUNK_HOME/etc/system/default/server.conf

Answer: AB

Reference: https://docs.splunk.com/Documentation/Splunk/7.3.2/Indexer/Enableclustersindetail

Question: 83

A Splunk architect has inherited the Splunk deployment at Buttercup Games and end users are complaining that the events are inconsistently formatted for a web sourcetype. Further investigation reveals that not all web logs flow through the same infrastructure: some of the data goes through heavy forwarders and some of the forwarders are managed by another department.
Which of the following items might be the cause for this issue?

A. The search head may have different configurations than the indexers.
B. The data inputs are not properly configured across all the forwarders.
C. The indexers may have different configurations than the heavy forwarders.
D. The forwarders managed by the other department are an older version than the rest.

Answer: D

Question: 84

A customer has installed a 500GB Enterprise license. They also purchased and installed a 300GB, no enforcement license on the same license master. How much data can the customer ingest before search is locked out?

A. 300GB. After this limit, search is locked out.
B. 500GB. After this limit, search is locked out.
C. 800GB. After this limit, search is locked out.
D. Search is not locked out. Violations are still recorded.

Answer: D

Reference: https://docs.splunk.com/Documentation/Splunk/7.3.2/Admin/TypesofSplunklicenses

Question: 85

What does the deployer do in a Search Head Cluster (SHC)? (Select all that apply.)
A. Distributes apps to SHC members.
B. Bootstraps a clean Splunk install for a SHC.
C. Distributes non-search related and manual configuration file changes.
D. Distributes runtime knowledge object changes made by users across the SHC.

Answer: A

Reference: https://docs.splunk.com/Documentation/Splunk/7.3.2/DistSearch/SHCdeploymentoverview

Question: 86

When using the props.conf LINE_BREAKER attribute to delimit multi-line events, the SHOULD_LINEMERGE attribute should be set to what?
A. Auto
B. None
C. True
D. False

Answer: C

Reference: https://answers.splunk.com/answers/6926/how-to-keep-data-together-as-one-event.html

Question: 87

Which of the following should be included in a deployment plan?
A. Business continuity and disaster recovery plans.
B. Current logging details and data source inventory.
C. Current and future topology diagrams of the IT environment.
D. A comprehensive list of stakeholders, either direct or indirect.

Answer: D

Reference: https://docs.splunk.com/Documentation/CoE/ssf/Handbook/StakeholderReg

Question: 88

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

Answer: D

Reference: https://docs.splunk.com/Documentation/Splunk/7.3.2/Indexer/Systemrequirements

Question: 89

Stakeholders have identified high availability for searchable data as their top priority. Which of the following best addresses this requirement?

A. Increasing the search factor in the cluster.
B. Increasing the replication factor in the cluster.
C. Increasing the number of search heads in the cluster.
D. Increasing the number of CPUs on the indexers in the cluster.

Answer: B

Reference: https://docs.splunk.com/Documentation/Splunk/7.3.2/DistSearch/SHCarchitecture

Question: 90

Search dashboards in the Monitoring Console indicate that the distributed deployment is approaching its capacity. Which of the following options will provide the most search performance improvement?

A. Replace the indexer storage to solid state drives (SSD).
B. Add more search heads and redistribute users based on the search type.
C. Look for slow searches and reschedule them to run during an off-peak time.
D. Add more search peers and make sure forwarders distribute data evenly across all indexers.

Answer: C