



**Vendor:** Splunk

**Exam Code:** SPLK-2002

**Exam Name:** Splunk Enterprise Certified Architect

**Version:** DEMO

#### QUESTION 1

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:** BC

**Explanation:**

Configure multisite nodes

To deploy and configure multisite cluster nodes, you must directly edit `server.conf` or use the CLI.

You cannot use Splunk Web.

#### QUESTION 2

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:** BCD

**Explanation:**

ANNOTATE\_PUNCT (AP) and SHOULD\_LINEMERGE (LM) which goes hand-in-hand with LINE\_BREAKER (LB).

See chapter "Tune `props.conf`" of *Architecting Splunk Enterprise Deployment*. The best indexing pipelines test results are when AP and LM (so LB too) are configured.

#### QUESTION 3

Which of the following are client filters available in `serverclass.conf`? (Select all that apply.)

- A. DNS name.
- B. IP address.
- C. Splunk server role.
- D. Platform (machine type).

**Answer:** ABD

**Explanation:**

# filters can be based on DNS name, IP address, build number of client

# machines, platform, and the clientName. If a target machine

# matches the filter, then the deployment server deploys the apps and configuration

# content that make up the server class to that machine.

#### QUESTION 4

What log file would you search to verify if you suspect there is a problem interpreting a regular expression in a monitor stanza?

- A. `btool.log`
- B. `metrics.log`

- C. splunkd.log
- D. tailing\_processor.log

**Answer: C**

**Explanation:**

The primary log for the Splunk server. The log is often requested by Splunk Support for troubleshooting purposes.

<https://docs.splunk.com/Documentation/Splunk/8.2.1/Troubleshooting/WhatSplunklogsaboutitself>

#### QUESTION 5

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**

**Explanation:**

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

#### QUESTION 6

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: B**

**Explanation:**

This attribute specifies the per-site searchable copy policy. It is specified globally and applies to all buckets in all indexes.

<https://docs.splunk.com/Documentation/Splunk/9.0.5/Indexer/Sitesearchfactor>

#### QUESTION 7

Which Splunk Enterprise offering has its own license?

- A. Splunk Cloud Forwarder
- B. Splunk Heavy Forwarder
- C. Splunk Universal Forwarder
- D. Splunk Forwarder Management

**Answer: C**

**Explanation:**

<https://docs.splunk.com/Splexicon:Forwardinglicense#:~:text=Splunk%20Enterprise%20offers%20several%20forwarder,package%20includes%20its%20own%20license.>

#### QUESTION 8

Which component in the splunkd.log will log information related to bad event breaking?

- A. Audittrail
- B. EventBreaking
- C. IndexingPipeline
- D. AggregatorMiningProcessor

**Answer: D**

**Explanation:**

Splunk Name, spelunking is the hobby of exploring caves and mines. Splunking, then, is the exploration of information caves and the mining of data.

<https://docs.splunk.com/Documentation/Splunk/8.2.4/Data/Resolvedataqualityissues>

#### QUESTION 9

Which Splunk server role regulates the functioning of indexer cluster?

- A. Indexer
- B. Deployer
- C. Master Node
- D. Monitoring Console

**Answer: C**

**Explanation:**

<https://docs.splunk.com/Documentation/Splunk/8.2.4/Deploy/Indexercluster>

<https://docs.splunk.com/Documentation/Splunk/8.2.4/Indexer/Enablethemanagernode>

#### QUESTION 10

When adding or rejoining a member to a search head cluster, the following error is displayed:

```
Error pulling configurations from the search head cluster captain;
consider performing a destructive configuration resync on this search
head cluster member.
```

What corrective action should be taken?

- A. Restart the search head.
- B. Run the splunk apply shcluster-bundle command from the deployer.
- C. Run the clean raft command on all members of the search head cluster.
- D. Run the splunk resync shcluster-replicated-config command on this member.

**Answer: D**

**Explanation:**

<https://community.splunk.com/t5/Deployment-Architecture/How-to-resolve-error-quot-Error-pulling-configurations-from-the/m-p/354231>

#### QUESTION 11

Which of the following commands is used to clear the KV store?

- A. splunk clean kvstore
- B. splunk clear kvstore

- C. splunk delete kvstore
- D. splunk reinitialize kvstore

**Answer: A**

**Explanation:**

<https://docs.splunk.com/Documentation/Splunk/8.2.4/Admin/ResyncKVstore>

#### QUESTION 12

Indexing is slow and real-time search results are delayed in a Splunk environment with two indexers and one search head. There is ample CPU and memory available on the indexers. Which of the following is most likely to improve indexing performance?

- A. Increase the maximum number of hot buckets in indexes.conf
- B. Increase the number of parallel ingestion pipelines in server.conf
- C. Decrease the maximum size of the search pipelines in limits.conf
- D. Decrease the maximum concurrent scheduled searches in limits.conf

**Answer: B**

**Explanation:**

<https://conf.splunk.com/files/2016/slides/harnessing-performance-and-scalability-with-parallelization.pdf>

#### QUESTION 13

The guidance Splunk gives for estimating size on for syslog data is 50% of original data size. How does this divide between files in the index?

- A. rawdata is: 10%, tsidx is: 40%
- B. rawdata is: 15%, tsidx is: 35%
- C. rawdata is: 35%, tsidx is: 15%
- D. rawdata is: 40%, tsidx is: 10%

**Answer: B**

**Explanation:**

<https://docs.splunk.com/Documentation/Splunk/8.2.4/Capacity/Estimateyourstoragerequirements>

#### QUESTION 14

A three-node search head cluster is skipping a large number of searches across time. What should be done to increase scheduled search capacity on the search head cluster?

- A. Create a job server on the cluster.
- B. Add another search head to the cluster.
- C. server.conf captain\_is\_adhoc\_searchhead = true.
- D. Change limits.conf value for max\_searches\_per\_cpu to a higher value.

**Answer: B**

**Explanation:**

Jacking up the max\_searches\_per\_cpu doesn't always solve the problem. There a limit to this strategy. Once you're out of cpu, its going to have large queue and skipped searches.

#### QUESTION 15

The frequency in which a deployment client contacts the deployment server is controlled by what?

- A. polling\_interval attribute in outputs.conf
- B. phoneHomeIntervalInSecs attribute in outputs.conf
- C. polling\_interval attribute in deploymentclient.conf
- D. phoneHomeIntervalInSecs attribute in deploymentclient.conf

**Answer:** D

**Explanation:**

<https://docs.splunk.com/Documentation/Splunk/8.2.4/Admin/Deploymentclientconf>

#### QUESTION 16

To activate replication for an index in an indexer cluster, what attribute must be configured in indexes.conf on all peer nodes?

- A. repFactor = 0
- B. replicate = 0
- C. repFactor = auto
- D. replicate = auto

**Answer:** C

**Explanation:**

<https://docs.splunk.com/Documentation/Splunk/8.2.4/Indexer/Configurethepeerindexes>

#### QUESTION 17

Which of the following clarification steps should be taken if apps are not appearing on a deployment client? (Select all that apply.)

- A. Check serverclass.conf of the deployment server.
- B. Check deploymentclient.conf of the deployment client.
- C. Check the content of SPLUNK\_HOME/etc/apps of the deployment server.
- D. Search for relevant events in splunkd.log of the deployment server.

**Answer:** ABD

**Explanation:**

There is no link between the etc/apps folder and deployment apps on the deployment server.

## Thank You for Trying Our Product

### Passleader Certification Exam Features:

- ★ More than **99,900** Satisfied Customers Worldwide.
- ★ Average **99.9%** Success Rate.
- ★ **Free Update** to match latest and real exam scenarios.
- ★ **Instant Download** Access! No Setup required.
- ★ Questions & Answers are downloadable in **PDF** format and **VCE** test engine format.
- ★ Multi-Platform capabilities - **Windows, Laptop, Mac, Android, iPhone, iPod, iPad**.
- ★ **100%** Guaranteed Success or **100%** Money Back Guarantee.
- ★ **Fast**, helpful support **24x7**.



View list of all certification exams: <http://www.passleader.com/all-products.html>



Microsoft



ORACLE



CITRIX



JUNIPER  
NETWORKS



EMC<sup>2</sup>  
where information lives

**10% Discount Coupon Code: ASTR14**