# ValidQuestions.com

# Splunk

## SPLK-1003 Exam

**Splunk Enterprise Certified Admin Exam**

## Questions & Answers
## (Demo Version – Limited Content)

Thank you for Downloading SPLK-1003 exam PDF Demo

Get Full File:
https://validquestions.com/exam/splunk-splk-1003/

# Version: 9.0

## Question: 1

Which setting in indexes. conf allows data retention to be controlled by time?

A. maxDaysToKeep
B. moveToFrozenAfter
C. maxDataRetentionTime
D. frozenTimePeriodlnSecs

**Answer: D**

Explanation:
https://docs.splunk.com/Documentation/Splunk/latest/Indexer/Setaretirementandarchivingpolicy

## Question: 2

The universal forwarder has which capabilities when sending data? (select all that apply)

A. Sending alerts
B. Compressing data
C. Obfuscating/hiding data
D. Indexer acknowledgement

**Answer: BD**

Explanation:
https://docs.splunk.com/Documentation/Splunk/8.0.1/Forwarding/Aboutforwardingandreceivingdata

## Question: 3

In case of a conflict between a whitelist and a blacklist input setting, which one is used?

A. Blacklist
B. Whitelist
C. They cancel each other out.
D. Whichever is entered into the configuration first.

**Answer: A**

Explanation:
https://docs.splunk.com/Documentation/Splunk/8.0.4/Data/Whitelistorblacklistspecificincomingdata

## Question: 4

In which Splunk configuration is the SEDCMD used?

A. props, conf
B. inputs.conf
C. indexes.conf
D. transforms.conf

**Answer: A**

Explanation:
https://docs.splunk.com/Documentation/Splunk/8.0.5/Forwarding/Forwarddatatothird-partysystemsd

## Question: 5

Which of the following are supported configuration methods to add inputs on a forwarder? (select all that apply)

A. CLI
B. Edit inputs . conf
C. Edit forwarder.conf
D. Forwarder Management

**Answer: ABD**

## Question: 6

Which parent directory contains the configuration files in Splunk?

A. SSFLUNK_KOME/etc
B. SSPLUNK_HCME/var
C. SSPLUNK_HOME/conf
D. SSPLUNK_HOME/default

**Answer: A**

## Question: 7

Which forwarder type can parse data prior to forwarding?

A. Universal forwarder
B. Heaviest forwarder
C. Hyper forwarder
D. Heavy forwarder

**Answer: D**

## Question: 8

Which Splunk component consolidates the individual results and prepares reports in a distributed environment?

A. Indexers
B. Forwarder
C. Search head
D. Search peers

**Answer: C**

## Question: 9

Which Splunk component distributes apps and certain other configuration updates to search head cluster members?

A. Deployer
B. Cluster master
C. Deployment server
D. Search head cluster master

**Answer: A**

## Question: 10

Where should apps be located on the deployment server that the clients pull from?

A. $SFLUNK_KOME/etc/apps

B. $SPLUNK_HCME/etc/sear:ch
C. $SPLUNK_HCME/etc/master-apps
D. $SPLUNK HCME/etc/deployment-apps

**Answer: D**

**Thank You for trying SPLK-1003 PDF Demo**

https://validquestions.com/exam/splunk-splk-1003/

Start Your SPLK-1003 Preparation

*[Limited Time Offer]* Use Coupon "dumps20" for extra 20% discounton the purchase of PDF Test your SPLK-1003 preparation with actual exam questions.