Splunk SPLK-1003 Practice Questions

Shared by Boyle on 18-08-2026

For More Free Questions and Preparation Resources

Check the Links on Last Page

Question 1

Question Type: MultipleChoice

An organization wants to collect Windows performance data from a set of clients, however, installing Splunk

software on these clients is not allowed. What option is available to collect this data in Splunk Enterprise?

Options:

A- Use Local Windows host monitoring.
B- Use Windows Remote Inputs with WMI.
C- Use Local Windows network monitoring.
D- Use an index with an Index Data Type of Metrics.

Answer:

B

Explanation:

https://docs.splunk.com/Documentation/Splunk/8.1.0/Data/ConsiderationsfordecidinghowtomonitorWindowsdata

'The Splunk platform collects remote Windows data for indexing in one of two ways: From Splunk forwarders, Using Windows Management Instrumentation (WMI). For Splunk Cloud deployments, you must use the Splunk Universal Forwarder on a Windows machines to montior remote Windows data.'

Question 2

Question Type: MultipleChoice

Which option best are methods for adding inputs in Splunk? (select all that apply)

Options:

A- CLI

B- Splunk Web
C- Editing inputs. conf
D- Editing monitor. conf

Answer:

A, B, C

Question 3

Question Type: MultipleChoice

When should the Data Preview feature be used?

Options:

A- When extracting fields for ingested data.
B- When previewing the data before searching.
C- When reviewing data on the source host.
D- When validating the parsing of data.

Answer:

D

Question 4

Question Type: MultipleChoice

How can native authentication be disabled in Splunk?

Options:

A- Remove the $SPLUNK_HOME/etc/passwd file
B- Create an empty $SPLUNK_HOME/etc/passwd file
C- Set SPLUNK_AUTHENTICATION=false in splunk-launch.conf
D- Set nativeAuthentication=false in authentication.conf

Answer:

B

Question 5

Question Type: MultipleChoice

A company moves to a distributed architecture to meet the growing demand for the use of Splunk. What parameter can be configured to enable automatic load balancing in the

Universal Forwarder to send data to the indexers?

Options:

A- Create one outputs . conf file for each of the server addresses in the indexing tier.
B- Configure the outputs . conf file to point to any server in the indexing tier and Splunk will configure the data to be sent to all of the indexers.
C- Splunk does not do load balancing and requires a hardware load balancer to balance traffic across the indexers.
D- Set the stanza to have a server value equal to a comma-separated list of IP addresses and indexer ports for each of the indexers in the environment.

Answer:

D

Question 6

Question Type: MultipleChoice

User role inheritance allows what to be inherited from the parent role? (select all that apply)

Options:

A- Parents
B- Capabilities
C- Index access
D- Search history

Answer:

B, C

Question 7

Question Type: MultipleChoice

Which of the following statements apply to directory inputs? {select all that apply)

Options:

A- All discovered text files are consumed.
B- Compressed files are ignored by default
C- Splunk recursively traverses through the directory structure.
D- When adding new log files to a monitored directory, the forwarder must be restarted to take them into account.

Answer:

A, C

Question 8

Question Type: MultipleChoice

Consider a company with a Splunk distributed environment in production. The Compliance Department wants to start using Splunk; however, they want to ensure that no one can see their reports or any other knowledge objects. Which Splunk Component can be added to implement this policy for the new team?

Options:

A- Indexer
B- Deployment server
C- Universal forwarder
D- Search head

Answer:

D

Question 9

Question Type: MultipleChoice

Which of the following lists the three phases of the Splunk Indexing process in order?

Options:

A- Ingest phaseLicensing phaseParsing phase
B- Sourcetype phaseIndex phaseWrite-to-disk phase
C- Input phaseParsing phaseIndexing phase
D- Ingest phaseTransforming phaseIndexing phase

Answer:

C

Explanation:

The Splunk indexing process consists of three main phases: Input, Parsing, and Indexing. Understanding these phases is crucial for configuring data inputs and managing data flow within Splunk.

Input Phase: Splunk receives data from various sources, such as files, network ports, or scripted inputs.

Parsing Phase: Splunk breaks the data into individual events, applies transformations, and extracts timestamps.

Indexing Phase: Splunk writes the parsed events to disk and creates indexes for efficient searching.

From the official Splunk documentation:

'The data pipeline consists of three main phases: input, parsing, and indexing.'

--- How the Splunk platform indexes data - Splunk Documentation

Therefore, the correct order of the indexing process is: Input phase Parsing phase Indexing phase.

How the Splunk platform indexes data - Splunk Documentation