# Exam Questions SPLK-1005

Splunk Cloud Certified Admin

**https://www.2passeasy.com/dumps/SPLK-1005/**

**NEW QUESTION 1**
Which configuration file determines how a universal forwarder forwards data to the indexer?

A. inputs.conf
B. outputs.conf
C. props.conf
D. transforms.conf

**Answer:** B

**NEW QUESTION 2**
Which feature of forwarders can protect the data from unauthorized access or tampering?

A. Data compression
B. SSL security
C. Data masking
D. Data encryption

**Answer:** B

**NEW QUESTION 3**
Which configuration file parameter can be used to modify line termination settings interactively, using the Set Source Type page in Splunk Web?

A. LINE_BREAKER
B. SHOULD_LINEMERGE
C. BREAK_ONLY_BEFORE
D. TRUNCATE

**Answer:** B

**NEW QUESTION 4**
Which option can be used to specify the source type of the data when creating a file or directory monitor input?

A. Set Source Type
B. Select Source Type
C. Choose Source Type
D. Define Source Type

**Answer:** A

**NEW QUESTION 5**
Which command can be used to download and install the universal forwarder software on a Linux system?

A. wget -O splunkforwarder-<version>-Linux-x86_64.tgz 'https://www.splunk.com/bin/splunk/DownloadActivityServlet?architecture=x86_64&platform=linux&ve
B. tar xvzf splunkforwarder-<version>-Linux-x86_64.tgz -C /opt
C. /opt/splunkforwarder/bin/splunk start --accept-license
D. All of the above

**Answer:** D

**NEW QUESTION 6**
Which type of forwarder is a full Splunk Enterprise instance that can run apps and add-ons?

A. Universal forwarder
B. Heavy forwarder
C. Deployment server
D. Search head

**Answer:** B

**NEW QUESTION 7**
What is the name of the Splunk Cloud setting that allows you to specify the maximum amount of raw data allowed before data is removed from the index?

A. Max raw data size
B. Max data retention
C. Max index size
D. Max data volume

**Answer:** A

**NEW QUESTION 8**
What is the name of the dashboard that provides information on incoming data consumption and indexing rate for your Splunk Cloud Platform deployment?

A. Indexing Performance
B. Indexing Quality
C. Indexing Status
D. Indexing Overview

**Answer:** A

**NEW QUESTION 9**
What is the name of the Splunk Enterprise feature that provides a security data and event management (SIEM) solution that uses machine data to detect and respond to threats?

A. Splunk Enterprise Security
B. Splunk Enterprise Intelligence
C. Splunk Enterprise Analytics
D. Splunk Enterprise Monitoring

**Answer:** A

**NEW QUESTION 10**
What is the name of the process that breaks the stream of raw data into individual lines called events?

A. Line breaking
B. Event annotation
C. Event transformation
D. Timestamp extraction

**Answer:** A

**NEW QUESTION 10**
What is the main difference between events indexes and metrics indexes in Splunk Cloud?

A. Events indexes impose minimal structure and can accommodate any kind of data, while metrics indexes use a highly structured format to handle metrics data.
B. Events indexes use a highly structured format to handle event-based log data, while metrics indexes impose minimal structure and can accommodate any kind of data.
C. Events indexes store data in compressed form, while metrics indexes store data in uncompressed form.
D. Events indexes store data in uncompressed form, while metrics indexes store data in compressed form.

**Answer:** A

**NEW QUESTION 15**
Which setting in inputs.conf can be used to specify the interval at which the script runs for a scripted input?

A. interval
B. frequency
C. schedule
D. cron

**Answer:** A

**NEW QUESTION 19**
What is the name of the configuration file that governs data inputs such as forwarders and file system monitoring?

A. inputs.conf
B. props.conf
C. transforms.conf
D. outputs.conf

**Answer:** A

**NEW QUESTION 22**
What is the name of the tab in Splunk Web where you can set the indexes that a role can access?

A. Inheritance
B. Capabilities
C. Indexes
D. Restrictions

**Answer:** C

**NEW QUESTION 27**
What is the name of the component that acts as a data manager and sends data to Splunk Cloud Platform indexers?

A. Heavy forwarder
B. Universal forwarder
C. Deployment server

D. License master

**Answer:** A

**NEW QUESTION 31**
Which file processor can be used to index files that are not actively written to or updated?

A. Monitor
B. MonitornoHandle
C. Upload
D. None of the above

**Answer:** C

**NEW QUESTION 35**
Which Windows-specific input type allows Splunk software to read special Windows log files such as the DNS debug server log?

A. MonitorNoHandle
B. Windows Event Log
C. Windows Registry
D. Windows Management Instrumentation (WMI)

**Answer:** A

**NEW QUESTION 39**
What is the name of the configuration file where you can set custom rules for event line breaking and line merging for a specific app?

A. inputs.conf
B. outputs.conf
C. props.conf
D. transforms.conf

**Answer:** C

**NEW QUESTION 42**
What is the name of the configuration file that you need to edit to enable Data Preview for the search app?

A. limits.conf
B. props.conf
C. inputs.conf
D. outputs.conf

**Answer:** A

**NEW QUESTION 46**
What is the name of the configuration file where you can invoke data transformations by associating them with a host, source, or source type?

A. limits.conf
B. props.conf
C. inputs.conf
D. transforms.conf

**Answer:** B

**NEW QUESTION 51**
Which command can be used to install the Splunk universal forwarder credentials package on the universal forwarder machine?

A. splunk install app <path_to_credentials_package>
B. splunk add app <path_to_credentials_package>
C. splunk install forwarder-credentials <path_to_credentials_package>
D. splunk add forwarder-credentials <path_to_credentials_package>

**Answer:** A

**NEW QUESTION 56**
.....

# THANKS FOR TRYING THE DEMO OF OUR PRODUCT

Visit Our Site to Purchase the Full Set of Actual SPLK-1005 Exam Questions With Answers.

We Also Provide Practice Exam Software That Simulates Real Exam Environment And Has Many Self-Assessment Features. Order the SPLK-1005 Product From:

**https://www.2passeasy.com/dumps/SPLK-1005/**

## Money Back Guarantee

**SPLK-1005 Practice Exam Features:**

* SPLK-1005 Questions and Answers Updated Frequently

* SPLK-1005 Practice Questions Verified by Expert Senior Certified Staff

* SPLK-1005 Most Realistic Questions that Guarantee you a Pass on Your FirstTry

* SPLK-1005 Practice Test Questions in Multiple Choice Formats and Updatesfor 1 Year