# Splunk

## Exam Questions SPLK-1005

Splunk Cloud Certified Admin

# About Exambible

## *Your Partner of IT Exam*

## Found in 1998

Exambible is a company specialized on providing high quality IT exam practice study materials, especially Cisco CCNA, CCDA, CCNP, CCIE, Checkpoint CCSE, CompTIA A+, Network+ certification practice exams and so on. We guarantee that the candidates will not only pass any IT exam at the first attempt but also get profound understanding about the certificates they have got. There are so many alike companies in this industry, however, Exambible has its unique advantages that other companies could not achieve.

## Our Advances

* 99.9% Uptime

All examinations will be up to date.

* 24/7 Quality Support

We will provide service round the clock.

* 100% Pass Rate

Our guarantee that you will pass the exam.

* Unique Gurantee

If you do not pass the exam at the first time, we will not only arrange FULL REFUND for you, but also provide you another exam of your claim, ABSOLUTELY FREE!

**NEW QUESTION 1**
What is the default value of the LINE_BREAKER setting that splits the incoming stream of data into separate lines?

A. Any sequence of newlines and carriage returns
B. Any sequence of spaces and tabs
C. Any sequence of punctuation marks
D. Any sequence of alphanumeric characters

**Answer:** A

**NEW QUESTION 2**
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 3**
Which option in Splunk Web can be used to create a new local TCP input?

A. Settings > Data Inputs > TCP > New Local TCP
B. Settings > Data Inputs > TCP > Add New
C. Settings > Data Inputs > TCP > Create New
D. Settings > Data Inputs > TCP > New Data Input

**Answer:** A

**NEW QUESTION 4**
What is the name of the attribute that specifies the sed script for data transformation in the props.conf file?

A. SEDCMD
B. FORMAT
C. DEST_KEY
D. TRANSFORMS

**Answer:** A

**NEW QUESTION 5**
What is the name of the attribute that you need to set to true in the [search] stanza of the limits.conf file to enable Data Preview?

A. timeline_events_preview
B. data_preview_enabled
C. show_data_preview
D. enable_data_preview

**Answer:** A

**NEW QUESTION 6**
What is the name of the configuration file where you can define data transformations using regular expressions and other attributes?

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

**Answer:** D

**NEW QUESTION 7**
Which setting in inputs.conf can be used to specify the SSL certificate for a TCP or UDP input?

A. sslCertPath
B. sslRootCAPath
C. sslPassword
D. All of the above

**Answer:** D

**NEW QUESTION 8**
Which option in Splunk web can be used to access the Guided Data On-boarding feature?

A. Add data
B. Data inputs
C. Data summary
D. Data models

**Answer:** A

**NEW QUESTION 9**
What is the name of the default field that stores the timestamps in UNIX time when data is indexed?

A. _time
B. _timestamp
C. _date
D. _epoch

**Answer:** A

**NEW QUESTION 10**
What are the three types of data that indexes contain in Splunk Cloud?

A. Raw data, index data, and metadata
B. Raw data, event data, and metadata
C. Raw data, index data, and event data
D. Raw data, index data, and metrics data

**Answer:** A

**NEW QUESTION 10**
Which input type can be used to monitor Windows Registry Values for changes?

A. WinRegMon
B. WinRegistry
C. WinRegValue
D. WinRegChange

**Answer:** A

**NEW QUESTION 12**
Which attribute in outputs.conf can be used to specify the load balancing method for a group of forwarders?

A. autoLB
B. autoLBFrequency
C. lb_method
D. lb_poll

**Answer:** C

**NEW QUESTION 17**
What is the main advantage of managed Splunk Cloud over self-service Splunk Cloud in terms of scalability and reliability?

A. Managed Splunk Cloud provides a single-instance environment that can scale up to 10TB/day and offers a 100% uptime SLA.
B. Managed Splunk Cloud provides a clustered environment that can scale up to 10TB/day and offers a 100% uptime SLA.
C. Managed Splunk Cloud provides a single-instance environment that can scale up to 5TB/day and offers a 99.9% uptime SLA.
D. Managed Splunk Cloud provides a clustered environment that can scale up to 5TB/day and offers a 99.9% uptime SLA.

**Answer:** B

**NEW QUESTION 18**
Which feature allows a light forwarder to reduce the amount of data sent to the indexer by discarding some events or fields?

A. Data cloning
B. Data filtering
C. Data sampling
D. Data masking

**Answer:** C

**NEW QUESTION 23**
Which configuration file needs to be edited to configure the universal forwarder to act as a deployment client?

A. deploymentclient.conf
B. server.conf
C. outputs.conf
D. inputs.conf

**Answer:** A

**NEW QUESTION 27**
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 30**
Which setting in inputs.conf can be used to set the host field to a static value for a monitor input?

A. host
B. host_regex
C. host_segment
D. host_override

**Answer:** A

**NEW QUESTION 33**
Which configuration file contains the settings for event line breaking and line merging?

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

**Answer:** C

**NEW QUESTION 38**
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 41**
What is the name of the directory that contains all the Splunk indexes and other important data??

A. /bin
B. /var
C. /etc
D. /lib

**Answer:** B

**NEW QUESTION 45**
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 47**
What is the name of the topology that allows you to initiate searches from an on-premises Splunk Enterprise search head to a single Splunk Cloud Platform deployment?

A. Hybrid Search Topology
B. Federated Search Topology
C. Distributed Search Topology
D. Clustered Search Topology

**Answer:** A

**NEW QUESTION 48**
What is the main advantage of self-service Splunk Cloud over managed Splunk Cloud in terms of cost and control?

A. Self-service Splunk Cloud costs less to get started and maintain and allows your organization total control in setup and security configurations.
B. Self-service Splunk Cloud costs more to get started and maintain but allows your organization total control in setup and security configurations.
C. Self-service Splunk Cloud costs less to get started and maintain but requires your organization to rely on Splunk for setup and security configurations.
D. Self-service Splunk Cloud costs more to get started and maintain and requires your organization to rely on Splunk for setup and security configurations.

**Answer:** A

**NEW QUESTION 49**
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 50**
What is the name of the first step that you need to perform to configure the LDAP authentication scheme with Splunk Web?

A. Create an LDAP strategy
B. Map LDAP groups to Splunk roles
C. Configure LDAP settings
D. Test LDAP connection

**Answer:** A

**NEW QUESTION 55**
Which type of forwarder can act as an intermediate forwarder to receive data from other forwarders and send it to the indexer?

A. Universal forwarder
B. Heavy forwarder
C. Light forwarder
D. Any type of forwarder

**Answer:** B

**NEW QUESTION 56**
Which command can be used to install a universal forwarder on a Linux system?

A. splunk install forwarder
B. splunk forwarder install
C. splunk add forward-server
D. splunk enable boot-start

**Answer:** A

**NEW QUESTION 57**
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 61**
Which Splunk add-on simplifies the process of getting data into Splunk Cloud Platform from Windows Event Log channels?

A. Splunk Add-on for Windows
B. Splunk Add-on for Infrastructure
C. Splunk Add-on for Active Directory
D. Splunk Add-on for DNS

**Answer:** A

**NEW QUESTION 62**
.....

# Relate Links

**100% Pass Your SPLK-1005 Exam with Exambible Prep Materials**

https://www.exambible.com/SPLK-1005-exam/

# Contact us

**We are proud of our high-quality customer service, which serves you around the clock 24/7.**

**Viste -** https://www.exambible.com/