

## SPLK-1005 Dumps

### Splunk Cloud Certified Admin

<https://www.certleader.com/SPLK-1005-dumps.html>



**NEW QUESTION 1**

What are the four default roles that Splunk Cloud Platform comes with?

- A. admin, power, user, can\_delete
- B. admin, power, user, sc\_admin
- C. admin, power, user, guest
- D. admin, power, user, can\_write

**Answer:** B

**NEW QUESTION 2**

What is the name of the attribute that specifies the name of the stanza in the transforms.conf file that defines the data transformation in the props.conf file?

- A. REGEX
- B. FORMAT
- C. DEST\_KEY
- D. TRANSFORMS

**Answer:** D

**NEW QUESTION 3**

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 4**

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 5**

What are the two options for Dynamic Data Storage in Splunk Cloud that allow you to move expired data from indexes to another storage location?

- A. Splunk Archive and Self Storage
- B. Splunk Backup and Self Storage
- C. Splunk Archive and Splunk Backup
- D. Self Storage and Splunk Restore

**Answer:** A

**NEW QUESTION 6**

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 7**

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 8**

Which setting in inputs.conf can be used to specify the maximum size of a file that can be monitored by Splunk?

- A. max\_file\_size
- B. max\_file\_age
- C. max\_file\_count
- D. max\_file\_bytes

**Answer:** A

**NEW QUESTION 9**

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 10**

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 10**

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 12**

Which type of forwarder is a legacy option that is not recommended for new deployments?

- A. Universal forwarder
- B. Heavy forwarder
- C. Light forwarder
- D. Deployment client

**Answer:** C

**NEW QUESTION 15**

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 16**

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 17**

.....

## Thank You for Trying Our Product

\* 100% Pass or Money Back

All our products come with a 90-day Money Back Guarantee.

\* One year free update

You can enjoy free update one year. 24x7 online support.

\* Trusted by Millions

We currently serve more than 30,000,000 customers.

\* Shop Securely

All transactions are protected by VeriSign!

**100% Pass Your SPLK-1005 Exam with Our Prep Materials Via below:**

<https://www.certleader.com/SPLK-1005-dumps.html>