SPLK-1005$^{\text{Q\&As}}$

Splunk Cloud Certified Admin

QUESTION 1

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

Correct Answer: A

QUESTION 2

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

Correct Answer: A

QUESTION 3

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

Correct Answer: A

QUESTION 4

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

Correct Answer: A

QUESTION 5

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

Correct Answer: A