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 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 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 3
Which command can be used to run a 'splunk diag' on both the indexer and the forwarder?

A. splunk diag -collect all -uri https://<username>:<password>@<host>:<port>
B. splunk diag -collect all -auth <username>:<password>
C. splunk diag -collect all -server <host>:<port>
D. splunk diag -collect all -user <username> -password <password>

Answer: B

NEW QUESTION 4
Which feature allows a heavy forwarder to route data to different indexers based on criteria such as source, sourcetype, or host?

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

Answer: A

NEW QUESTION 5
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 6
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 7
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 8
What is the name of the option that you need to check in Splunk Web to enable LDAP authentication for your Splunk Cloud Platform deployment?

A. LDAP
B. External
C. LDAP/External
D. External/LDAP

Answer: C

NEW QUESTION 9
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 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 10
What is the regular expression format that represents any sequence of newlines and carriage returns, which is the default value of the LINE_BREAKER setting?

A. ([\r\n]+)
B. ([\s]+)
C. ([\w]+)
D. ([\p]+)

Answer: A

NEW QUESTION 11
Which option can be used to specify the host value of the data when creating a file or directory monitor input?

A. Set Host
B. Select Host
C. Choose Host
D. Define Host

Answer: A

NEW QUESTION 16
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 20
Which type of forwarder has the lowest system resource usage and the highest data throughput?

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

Answer: A

NEW QUESTION 22
Which file processor can be used to index files that are locked by another process on Windows systems?

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

Answer: B

NEW QUESTION 25
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 27
......

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/