Splunk Certification

Certification Exam Study Guide

S¢v©xu Ce¥¨nknca¨nzx E°aw¦

Tabve zk Czx¨ex¨¦

- Splunk Core Certified User
  -

Please note: These sample questions are provided to give candidates a general idea of the formatting and type of questions for each of the exams listed above. The test blueprints (linked for each specific exam in the following pages) provide much more detailed information regarding exam content. Candidate performance on these questions in no way guarantees performance or passing marks on the certification exam(s).

S¢v©xu Ce¥¨nknca¨nzx E°aw¦

Saw¢ve Q©e¦¨nzx¦ Ý S¢v©xu Cz¥e Ce¥¨nkned U¦e¥

Fz¥ a de¨anved b¥eaudz¯x zk ¨me e°aw czx¨ex¨Ë ¢vea¦e ¦ee ¨me Splunk Core Certified User Test BlueprintÎ

1. Which of the following is a main processing component of basic Splunk architecture?
   a. Indexer
   b. Load balancer
   c. License master
   d. Deployment server

2. According to Splunk best practices, which of the following searches is most efficient if we are interested in searching the Windows Security Event Log for failures?
   a. `status=failure`
   b. `index=oswinsec sourcetype=WinEventLog:Security status=failure`
   c. `index=oswinsec sourcetype=WinEventLog:* status=failure`
   d. `index=oswinsec failure`

3. Which search command calculates statistics based on fields in the events?
   a. `top`

S¢v©xu Ce¥¨nknca¨nzx E°aw¦

Answer Key Ý S¢v©xu Cz¥e Ce¥¨nkned U¦e¥

Fz¥ a de¨anved b¥eaudz¯x zk ¨me e°aw czx¨ex¨Ë ¢vea¦e ¦ee ¨me Splunk Core Certified User Test BlueprintÎ

1. A
2. B
3. C

S¢v©xu Ce¥¨nknca¨nzx E°aw¦

Saw¢ve Q©e¦¨nzx¦ Ý S¢v©xu Cz¥e Ce¥¨nkned Pz¯e¥ U¦e¥

Fz¥ a de¨anved b¥eaudz¯x zk ¨me e°aw czx¨ex¨Ë ¢vea¦e ¦ee ¨me Splunk Core Certified Power User Test BlueprintÎ

1. Which command is used only to create a time series visualization?
   a. `_time`
   b. `chart`
   c. `timechart`
   d. `timeseries`

2. Which of the following statements describe field aliases? (select all that apply)
   a. Field aliases are applied after lookups.
   b. Field aliases can be applied to lookups.
   c. Multiple aliases can be applied to one field.
   d. The original field is not replaced by the field alias.

3. What action type is used when creating a POST workflow action?
   a. Web
   b. Link
   c. HTTP
   d. HTTPS

S¢v©xu Ce¥¨nknca¨nzx E°aw¦

S¢v©xu Ce¥¨nknca¨nzx E°aw¦

Saw¢ve Q©e¦¨nzx¦ Ý S¢v©xu Ex¨e¥¢¥n¦e Ce¥¨nkned Adwnx

Fz¥ a de¨anved b¥eaudz¯x zk ¨me e°aw czx¨ex¨Ë ¢vea¦e ¦ee ¨me Splunk Enterprise Certified Admin Test BlueprintÎ

1. Which Splunk component receives, indexes, and stores incoming data from forwarders?
   a. Indexer
   b. Search head
   c. Cluster master
   d. Deployment server

2. Which license type allows 500MB/day of indexing, but disables alerts, authentication, cluster, distributed search, summarization, and forwarding to non-Splunk servers?
   a. Free license
   b. Forwarder license
   c. Enterprise license
   d. Enterprise trial license

3. What can be used when setting the host field option on a network input? (select all that apply)
   a. IP

   c. A binary filster, distributed search,
   d. Custom (explicit value)

S¢v©xu Ce¥¨nknca¨nzx E°aw¦

Answer Key Ý S¢v©xu Ex¨e¥¢¥n¦e Ce¥¨nkned Adwnx

Fz¥ a de¨anved b¥eaudz¯x zk ¨me e°aw czx¨ex¨Ë ¢vea¦e ¦ee ¨me Splunk Enterprise Certified Admin Test BlueprintÎ

S¢v©xu Ce¥¨nknca¨nzx E°aw¦

Answer Key Ý S¢v©xu Ex¨e¥¢¥n¦e Ce¥¨nkned A¥cmn¨ec¨

Fz¥ a de¨anved b¥eaudz¯x zk ¨me e°aw czx¨ex¨Ë ¢vea¦e ¦ee ¨me