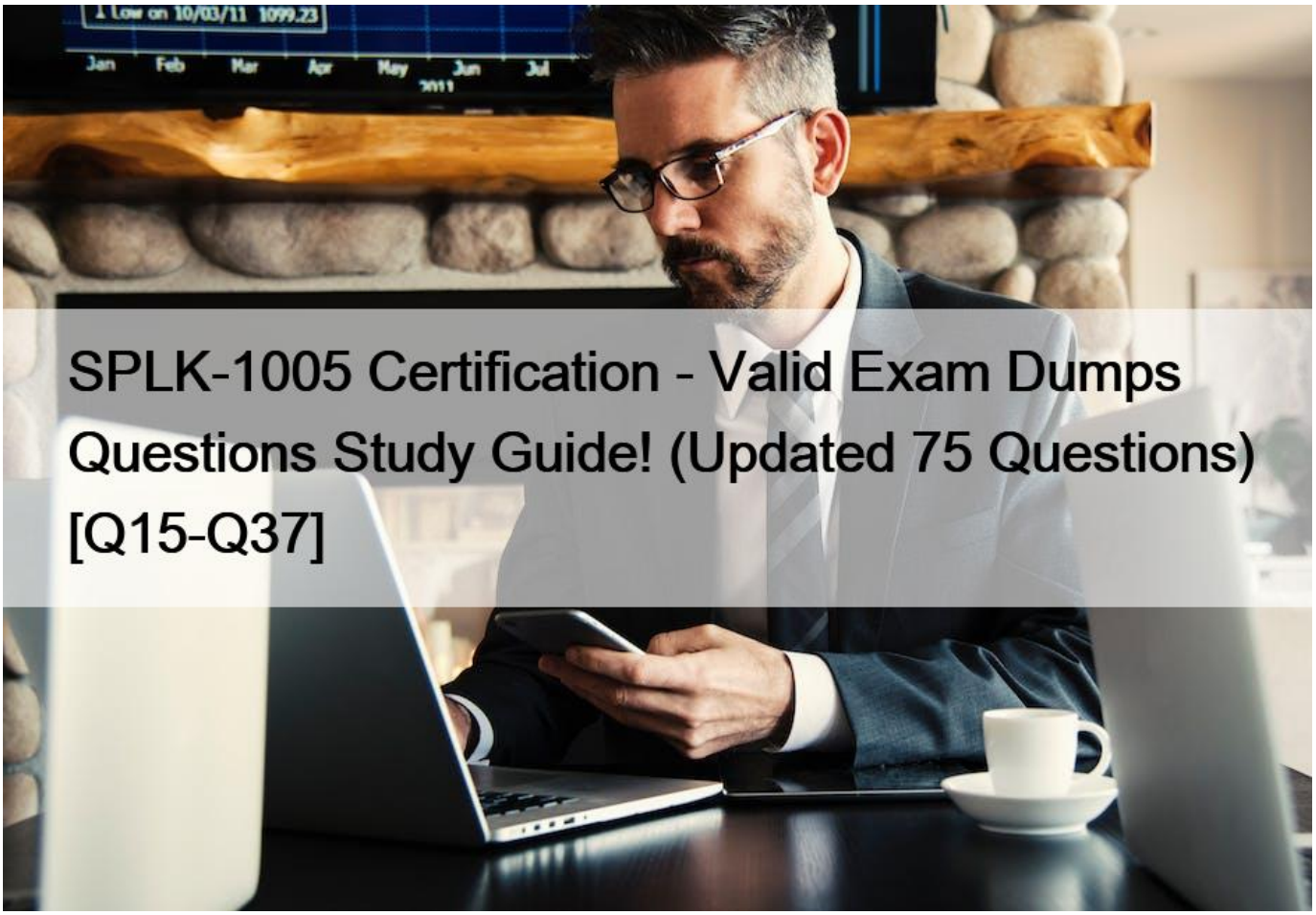
SPLK-1005 Certification - Valid Exam Dumps Questions Study Guide! (Updated 75 Questions) [Q15-Q37



SPLK-1005 Certification – Valid Exam Dumps Questions Study Guide! (Updated 75 Questions)
SPLK-1005 Dumps are Available for Instant Access using ValidExam

Splunk SPLK-1005 certification exam validates the knowledge and skills of administrators in managing Splunk Cloud environments. It tests a candidate's understanding of software-defined networking, index data, logs, metrics, and events. Additionally, it covers configurations related to data inputs, indexes, searches, and data management. SPLK-1005 exam also includes assessing a candidate's troubleshooting skills for issues related to configurations and scalability.

Earning the Splunk SPLK-1005 certification demonstrates a professional's expertise in managing and administering Splunk Cloud environments. It also validates their ability to effectively troubleshoot and maintain Splunk Cloud instances, ensuring that businesses can get the most out of their investment in the platform. Splunk Cloud Certified Admin certification can also help professionals advance their careers by demonstrating their knowledge and skills to potential employers.

QUESTION 15

What is the name of the Splunk Cloud feature that allows you to perform self-service administrative tasks such as creating indexes, inputs, and roles?
* Admin Config Service
* Admin Console
* Admin Dashboard
* Admin Toolkit

QUESTION 16

What is the name of the Splunk Cloud feature that allows you to monitor and manage resource utilization by business units and users using a Splunk app?
* Splunk App for Chargeback
* Splunk App for Resource Management
* Splunk App for Usage Analytics
* Splunk App for Cost Optimization

QUESTION 17

What are the four default roles that Splunk Cloud Platform comes with?
* admin, power, user, can_delete
* admin, power, user, sc_admin
* admin, power, user, guest
* admin, power, user, can_write

QUESTION 18

Which Windows-specific input type allows Splunk software to read special Windows log files such as the DNS debug server log?
* MonitorNoHandle
* Windows Event Log
* Windows Registry
* Windows Management Instrumentation (WMI)

QUESTION 19

Which feature of forwarders can prevent data loss in case of network failure or congestion?
* Data compression
* SSL security
* Configurable buffering
* Persistent queues

QUESTION 20

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?
* Max raw data size
* Max data retention
* Max index size
* Max data volume

QUESTION 21

Which command can be used to add a data input using the CLI?
* splunk add input
* splunk add monitor
* splunk add data
* splunk add source

QUESTION 22

Which file processor can be used to index files that are locked by another process on Windows systems?
* Monitor
* MonitornoHandle
* Upload
* None of the above

QUESTION 23

Which setting in inputs.conf can be used to set the host field to a static value for a monitor input?
* host
* host_regex
* host_segment
* host_override

QUESTION 24

Which configuration file parameter can be used to modify line termination settings interactively, using the Set Source Type page in Splunk Web?
* LINE_BREAKER
* SHOULD_LINEMERGE
* BREAK_ONLY_BEFORE
* TRUNCATE

QUESTION 25

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?
* Splunk Enterprise Security
* Splunk Enterprise Intelligence
* Splunk Enterprise Analytics
* Splunk Enterprise Monitoring

QUESTION 26

Which setting in inputs.conf can be used to specify the SSL certificate for a TCP or UDP input?
* sslCertPath
* sslRootCAPath
* sslPassword
* All of the above

QUESTION 27

Which configuration file contains the settings for event line breaking and line merging?
* inputs.conf
* outputs.conf
* props.conf
* transforms.conf

QUESTION 28

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?
* ([rn]+)
* ([s]+)
* ([w]+)
* ([p]+)

QUESTION 29

Which command can be used to run a ‘splunk diag’ on both the indexer and the forwarder?
* splunk diag -collect all -uri https://<username>:<password>@<host>:<port>
* splunk diag -collect all -auth <username>:<password>
* splunk diag -collect all -server <host>:<port>
* splunk diag -collect all -user <username> -password <password>

QUESTION 30

Which command can be used to install the Splunk universal forwarder credentials package on the universal forwarder machine?
* splunk install app <path_to_credentials_package>
* splunk add app <path_to_credentials_package>
* splunk install forwarder-credentials <path_to_credentials_package>
* splunk add forwarder-credentials <path_to_credentials_package>

QUESTION 31

Which input type can be used to monitor Windows Event Logs from a remote machine?
* WinEventLog
* WinEventLogCollections
* WinEventLogForwarder
* WinEventLogRemote

QUESTION 32

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?
* REGEX
* FORMAT
* DEST_KEY
* TRANSFORMS

QUESTION 33

What is the main advantage of managed Splunk Cloud over self-service Splunk Cloud in terms of scalability and reliability?
* Managed Splunk Cloud provides a single-instance environment that can scale up to 10TB/day and offers a 100% uptime SLA.
* Managed Splunk Cloud provides a clustered environment that can scale up to 10TB/day and offers a

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

99.9% uptime SLA.

QUESTION 34

Which command can be used to install a universal forwarder on a Linux system?
* splunk install forwarder
* splunk forwarder install
* splunk add forward-server
* splunk enable boot-start

QUESTION 35

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?
* inputs.conf
* outputs.conf
* props.conf
* transforms.conf

QUESTION 36

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?
* LDAP
* External
* LDAP/External
* External/LDAP

QUESTION 37

Which type of metadata can be used to identify the origin of the data?
* Source
* Source type
* Host
* Index

Splunk SPLK-1005 Exam Practice Test Questions: https://www.validexam.com/SPLK-1005-latest-dumps.html]