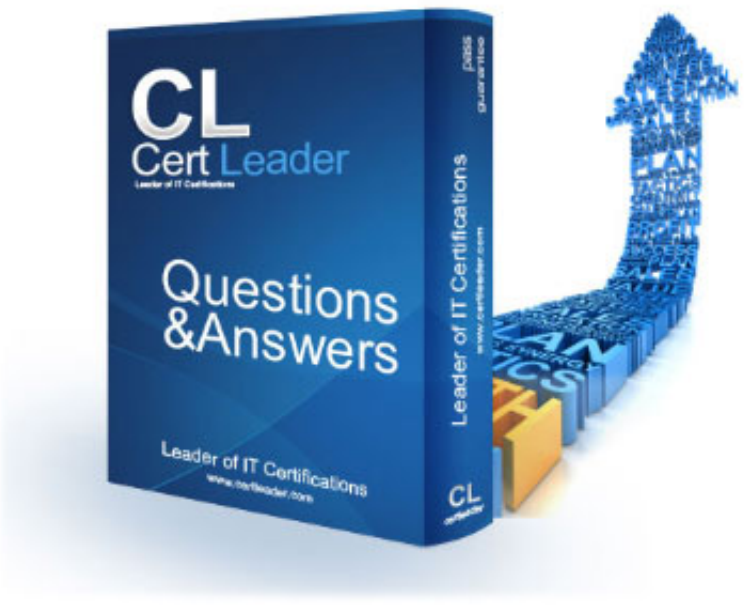
SPLK-1005 Dumps

Splunk Cloud Certified Admin

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



NEW QUESTION 1
What is the name of the attribute that specifies the sed script for data transformation in the props.conf file?

A. SEDCMD
B. FORMAT
C. DEST_KEY
D. TRANSFORMS

Answer: A

NEW QUESTION 2
Which feature of forwarders can protect the data from unauthorized access or tampering?

A. Data compression
B. SSL security
C. Data masking
D. Data encryption

Answer: B

NEW QUESTION 3
What is the name of the configuration file where you can define data transformations using regular expressions and other attributes?

A. limits.conf
B. props.conf
C. inputs.conf
D. transforms.conf

Answer: D

NEW QUESTION 4
Which configuration file needs to be edited to enable local indexing on the forwarder?

A. outputs.conf
B. inputs.conf
C. props.conf
D. transforms.conf

Answer: A

NEW QUESTION 5
Which setting in inputs.conf can be used to specify the SSL certificate for a TCP or UDP input?

A. sslCertPath
B. sslRootCAPath
C. sslPassword
D. All of the above

Answer: D

NEW QUESTION 6
Which network protocol is recommended for sending data to Splunk because it guarantees the delivery of network packets?

A. TCP
B. UDP
C. SNMP
D. ICMP

Answer: A

NEW QUESTION 7
Which setting in inputs.conf can be used to specify the command to run the script for a scripted input?

A. script
B. command
C. exec
D. run

Answer: C

NEW QUESTION 8
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 9
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 10
What is the name of the dashboard that provides information on incoming data consumption and indexing rate for your Splunk Cloud Platform deployment?

A. Indexing Performance
B. Indexing Quality
C. Indexing Status
D. Indexing Overview

Answer: A

NEW QUESTION 10
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 12
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?

A. Splunk App for Chargeback
B. Splunk App for Resource Management
C. Splunk App for Usage Analytics
D. Splunk App for Cost Optimization

Answer: A

NEW QUESTION 13
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 18
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

Answer: A

NEW QUESTION 23
Which tool can be used to verify that data is actually being received on the specified port on the indexing server?

A. tcpdump
B. netstat
C. ping
D. traceroute

Answer: A

NEW QUESTION 27
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 28
Which input type can be used to monitor Windows Event Logs from a remote machine?

A. WinEventLog
B. WinEventLogCollections
C. WinEventLogForwarder
D. WinEventLogRemote

Answer: B

NEW QUESTION 32
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 36
Which type of forwarder can perform data parsing and enrichment before sending it to the indexer?

A. Universal forwarder
B. Heavy forwarder
C. Deployment server
D. Search head

Answer: B

NEW QUESTION 41
Which type of metadata can be used to identify the origin of the data?

A. Source
B. Source type
C. Host
D. Index

Answer: C

NEW QUESTION 42
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 43
Which file processor can be used to index files that are not actively written to or updated?

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

Answer: C

NEW QUESTION 44
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 47
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?

A. inputs.conf
B. outputs.conf
C. props.conf
D. transforms.conf

Answer: C

NEW QUESTION 49
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 51
Which feature of forwarders can improve the network performance and reduce the bandwidth consumption?

A. Data compression
B. SSL security
C. Data sampling
D. Data filtering

Answer: A

NEW QUESTION 52
What is the name of the configuration file where you can invoke data transformations by associating them with a host, source, or source type?

A. limits.conf
B. props.conf
C. inputs.conf
D. transforms.conf

Answer: B

NEW QUESTION 56
Which command can be used to install the Splunk universal forwarder credentials package on the universal forwarder machine?

A. splunk install app <path_to_credentials_package>
B. splunk add app <path_to_credentials_package>
C. splunk install forwarder-credentials <path_to_credentials_package>
D. splunk add forwarder-credentials <path_to_credentials_package>

Answer: A

NEW QUESTION 57
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?

A. Admin Config Service
B. Admin Console
C. Admin Dashboard
D. Admin Toolkit

Answer: A

NEW QUESTION 58
.....

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