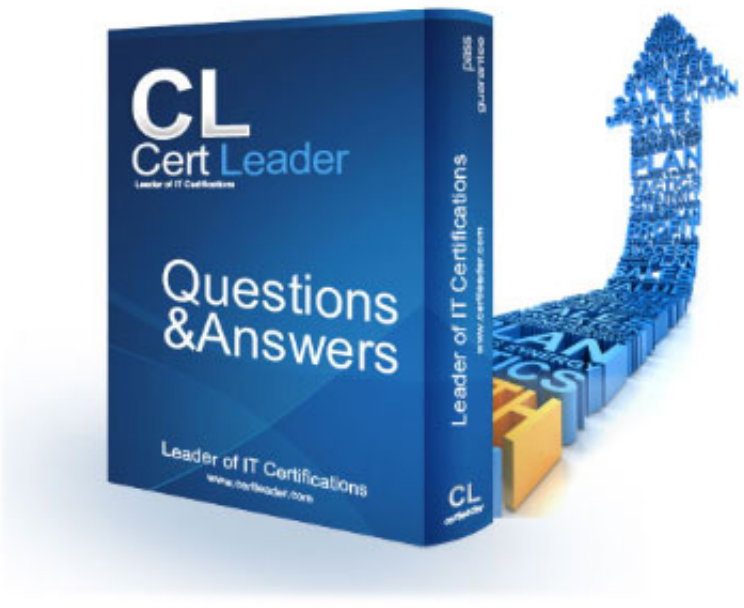
SPLK-1005 Dumps

Splunk Cloud Certified Admin

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



NEW QUESTION 1
Which configuration file determines how a universal forwarder forwards data to the indexer?

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

Answer: B

NEW QUESTION 2
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 3
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 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 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 7
Which command can be used to download and install the universal forwarder software on a Linux system?

A. wget -O splunkforwarder-<version>-Linux-x86_64.tgz ‘https://www.splunk.com/bin/splunk/DownloadActivityServlet?architecture=x86_64&platform=linux&ve
B. tar xvzf splunkforwarder-<version>-Linux-x86_64.tgz -C /opt
C. /opt/splunkforwarder/bin/splunk start --accept-license
D. All of the above

Answer: D

NEW QUESTION 8
What are the three types of data that indexes contain in Splunk Cloud?

A. Raw data, index data, and metadata
B. Raw data, event data, and metadata
C. Raw data, index data, and event data
D. Raw data, index data, and metrics data

Answer: A

NEW QUESTION 9
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 10
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 10
What is the main advantage of managed Splunk Cloud over self-service Splunk Cloud in terms of scalability and reliability?

A. Managed Splunk Cloud provides a single-instance environment that can scale up to 10TB/day and offers a 100% uptime SLA.
B. Managed Splunk Cloud provides a clustered environment that can scale up to 10TB/day and offers a 100% uptime SLA.
C. Managed Splunk Cloud provides a single-instance environment that can scale up to 5TB/day and offers a 99.9% uptime SLA.
D. Managed Splunk Cloud provides a clustered environment that can scale up to 5TB/day and offers a 99.9% uptime SLA.

Answer: B

NEW QUESTION 11
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 14
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 16
Which configuration file needs to be edited to configure the universal forwarder to act as a deployment client?

A. deploymentclient.conf
B. server.conf
C. outputs.conf
D. inputs.conf

Answer: A

NEW QUESTION 18
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 21
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 22
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 23
What is the main difference between events indexes and metrics indexes in Splunk Cloud?

A. Events indexes impose minimal structure and can accommodate any kind of data, while metrics indexes use a highly structured format to handle metrics data.
B. Events indexes use a highly structured format to handle event-based log data, while metrics indexes impose minimal structure and can accommodate any kind of data.
C. Events indexes store data in compressed form, while metrics indexes store data in uncompressed form.
D. Events indexes store data in uncompressed form, while metrics indexes store data in compressed form.

Answer: A

NEW QUESTION 26
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 configuration file contains the settings for event line breaking and line merging?

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

Answer: C

NEW QUESTION 36
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 38

Which command can be used to add a data input using the CLI?

A. splunk add input
B. splunk add monitor
C. splunk add data
D. splunk add source

Answer: B

NEW QUESTION 39
What is the name of the directory that contains all the Splunk indexes and other important data??

A. /bin
B. /var
C. /etc
D. /lib

Answer: B

NEW QUESTION 44
What is the name of the configuration file that governs data inputs such as forwarders and file system monitoring?

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

Answer: A

NEW QUESTION 45
Which type of forwarder is a legacy option that is not recommended for new deployments?

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

Answer: C

NEW QUESTION 50
What is the name of the component that acts as a data manager and sends data to Splunk Cloud Platform indexers?

A. Heavy forwarder
B. Universal forwarder
C. Deployment server
D. License master

Answer: A

NEW QUESTION 54
What is the main advantage of self-service Splunk Cloud over managed Splunk Cloud in terms of cost and control?

A. Self-service Splunk Cloud costs less to get started and maintain and allows your organization total control in setup and security configurations.
B. Self-service Splunk Cloud costs more to get started and maintain but allows your organization total control in setup and security configurations.
C. Self-service Splunk Cloud costs less to get started and maintain but requires your organization to rely on Splunk for setup and security configurations.
D. Self-service Splunk Cloud costs more to get started and maintain and requires your organization to rely on Splunk for setup and security configurations.

Answer: A

NEW QUESTION 59
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 60
Which Windows-specific input type allows Splunk software to read special Windows log files such as the DNS debug server log?

A. MonitorNoHandle
B. Windows Event Log
C. Windows Registry

D. Windows Management Instrumentation (WMI)

Answer: A

NEW QUESTION 63
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 68
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 69
What is the name of the time standard that is the basis for time and time zones worldwide and does not change for Daylight Saving Time (DST)?

A. GMT
B. UTC
C. PST
D. BST

Answer: B

NEW QUESTION 71
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 76
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 79
.....

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