



Splunk

Exam Questions SPLK-1005

Splunk Cloud Certified Admin

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

Which option in Splunk Web can be used to create a new local TCP input?

- A. Settings > Data Inputs > TCP > New Local TCP
- B. Settings > Data Inputs > TCP > Add New
- C. Settings > Data Inputs > TCP > Create New
- D. Settings > Data Inputs > TCP > New Data Input

Answer: A

NEW QUESTION 3

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 4

Which option can be used to specify the source type of the data when creating a file or directory monitor input?

- A. Set Source Type
- B. Select Source Type
- C. Choose Source Type
- D. Define Source Type

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 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 8

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 9

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 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

Which feature of forwarders can prevent data loss in case of network failure or congestion?

- A. Data compression
- B. SSL security
- C. Configurable buffering
- D. Persistent queues

Answer: D

NEW QUESTION 13

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 16

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 21

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 22

What is the name of the Splunk Cloud feature that allows you to get data from APIs and other remote data interfaces through scripted inputs?

- A. Splunk Cloud Data Connectors
- B. Splunk Cloud Data Integrations
- C. Splunk Cloud Data Collectors
- D. Splunk Cloud Data Sources

Answer: C

NEW QUESTION 26

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 30

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 33

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 36

Which command can be used to install a universal forwarder on a Linux system?

- A. splunk install forwarder
- B. splunk forwarder install
- C. splunk add forward-server
- D. splunk enable boot-start

Answer: A

NEW QUESTION 37

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 40

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 43

.....

Thank You for Trying Our Product

We offer two products:

1st - We have Practice Tests Software with Actual Exam Questions

2nd - Questons and Answers in PDF Format

SPLK-1005 Practice Exam Features:

- * SPLK-1005 Questions and Answers Updated Frequently
- * SPLK-1005 Practice Questions Verified by Expert Senior Certified Staff
- * SPLK-1005 Most Realistic Questions that Guarantee you a Pass on Your FirstTry
- * SPLK-1005 Practice Test Questions in Multiple Choice Formats and Updatesfor 1 Year

100% Actual & Verified — Instant Download, Please Click
[Order The SPLK-1005 Practice Test Here](#)