# Exam Questions SPLK-1003

Splunk Enterprise Certified Admin

**https://www.2passeasy.com/dumps/SPLK-1003/**

**NEW QUESTION 1**
The universal forwarder has which capabilities when sending data? (Select all that apply.)

A. Sending alerts
B. Compressing data
C. Obfuscating/hiding data
D. Indexer acknowledgement

**Answer:** D

**Explanation:**
Reference: https://docs.splunk.com/Documentation/Splunk/7.3.1/Forwarding/Typesofforwarders

**NEW QUESTION 2**
In which Splunk configuration is the SEDCMD used?

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

**Answer:** A

**Explanation:**
Reference: https://answers.splunk.com/answers/212128/why-sedcmd-configured-in-propsconf-is-working-duri.html

**NEW QUESTION 3**
Where should apps be located on the deployment server that the clients pull from?

A. $SPLUNK_HOME/etc/apps
B. $SPLUNK_HOME/etc/search
C. $SPLUNK_HOME/etc/master-apps
D. $SPLUNK_HOME/etc/deployment-apps

**Answer:** A

**Explanation:**
Reference: https://answers.splunk.com/answers/371099/how-to-configure-deployment-apps-to-push-to-client.html

**NEW QUESTION 4**
When running the command shown below, what is the default path in which deploymentserver.conf is created?
splunk set deploy-poll deployServer:port

A. SPLUNK_HOME/etc/deployment
B. SPLUNK_HOME/etc/system/local
C. SPLUNK_HOME/etc/system/default
D. SPLUNK_HOME/etc/apps/deployment

**Answer:** B

**Explanation:**
Reference: https://docs.splunk.com/Documentation/Splunk/7.3.1/Updating/Configuredeploymentclients

**NEW QUESTION 5**
When configuring monitor inputs with whitelists or blacklists, what is the supported method of filtering the lists?

A. Slash notation
B. Regular expression
C. Irregular expression
D. Wildcard-only expression

**Answer:** B

**Explanation:**
Reference: https://docs.splunk.com/Documentation/Splunk/7.3.1/Updating/Filterclients

**NEW QUESTION 6**
To set up a network input in Splunk, what needs to be specified?

A. File path.
B. Username and password.
C. Network protocol and port number.
D. Network protocol and MAC address.

**Answer:** A

**Explanation:**
Reference: http://dev.splunk.com/view/dev -guide/SP-CAAAE3A

**NEW QUESTION 7**
Which Splunk forwarder type allows parsing of data before forwarding to an indexer?

A. Universal forwarder
B. Parsing forwarder
C. Heavy forwarder
D. Advanced forwarder

**Answer:** C

**Explanation:**
Reference: https://docs.splunk.com/Documentation/SplunkCloud/7.2.6/Forwarding/Typesofforwarders

**NEW QUESTION 8**
Which of the following statements describe deployment management? (Select all that apply.)

A. Requires an Enterprise license.
B. Is responsible for sending apps to forwarders.
C. Once used, is the only way to manage forwarders.
D. Can automatically restart the host OS running the forwarder.

**Answer:** A

**NEW QUESTION 9**
During search time, which directory of configuration files has the highest precedence?

A. $SPLUNK_HOME/etc/system/local
B. $SPLUNK_HOME/etc/system/default
C. $SPLUNK_HOME/etc/apps/app1/local
D. $SPLUNK_HOME/etc/users/admin/local

**Answer:** C

**Explanation:**
Reference: https://docs.splunk.com/Documentation/Splunk/7.3.0/Admin/Wheretofindtheconfigurationfiles

**NEW QUESTION 10**
Within props.conf, which stanzas are valid for data modification? (Select all that apply.)

A. Host
B. Server
C. Source
D. Sourcetype

**Answer:** CD

**Explanation:**
Reference: https://answers.splunk.com/answers/3687/host-stanza-in-props-conf-not-being-honored-for-udp-514-data-sources.html

**NEW QUESTION 10**
What is the correct order of steps in Duo Multifactor Authentication?

A. * 1. Request Login* 2. Connect to SAML server* 3. Duo MFA* 4. Create User session* 5. Authentication Granted* 6. Log into Splunk
B. * 1. Request Login* 2. Duo MFA* 3. Authentication Granted* 4. Connect to SAML server* 5. Log into Splunk* 6. Create User session
C. * 1. Request Login* 2. Check authentication / group mapping* 3. Authentication Granted* 4. Duo MFA* 5. Create User session* 6. Log into Splunk
D. * 1. Request Login* 2. Duo MFA* 3. Check authentication / group mapping* 4. Create User session* 5. Authentication Granted* 6. Log into Splunk

**Answer:** C

**Explanation:**
Reference: https://docs.splunk.com/Documentation/Splunk/7.3.1/Security/ConfigureDuo

**NEW QUESTION 15**
How does the Monitoring Console monitor forwarders?

A. By pulling internal logs from forwarders.
B. By using the forwarder monitoring add-on.
C. With internal logs forwarded by forwarders.
D. With internal logs forwarder by deployment server.

**Answer:** A

**NEW QUESTION 20**
Which of the following are supported options when configuring optional network inputs?

A. Metadata override, sender filtering options, network input queues (quantum queues)
B. Metadata override, sender filtering options, network input queues (memory/persistent queues)
C. Filename override, sender filtering options, network output queues (memory/persistent queues)
D. Metadata override, receiver filtering options, network input queues (memory/persistent queues)

**Answer:** D

**NEW QUESTION 21**
What is the default character encoding used by Splunk during the input phase?

A. UTF-8
B. UTF-16
C. EBCDIC
D. ISO 8859

**Answer:** A

**Explanation:**
Reference: https://docs.splunk.com/Documentation/Splunk/7.3.1/Data/Configurecharactersetencoding

**NEW QUESTION 25**
Local user accounts created in Splunk store passwords in which file?

A. $SPLUNK_HOME/etc/passwd
B. $SPLUNK_HOME/etc/authentication
C. $SPLUNK_HOME/etc/users/passwd.conf
D. $SPLUNK_HOME/etc/users/authentication.conf

**Answer:** A

**Explanation:**
Reference: https://docs.splunk.com/Documentation/Splunk/7.3.1/Admin/User-seedconf

**NEW QUESTION 27**
For single line event sourcetypes, it is most efficient to set SHOULD_LINEMERGE
to what value?

A. True
B. False
C. <regex string>
D. Newline Character

**Answer:** B

**Explanation:**
Reference: https://answers.splunk.com/answers/704533/what-are-the-best-practices-for-defining-source-ty.html

**NEW QUESTION 32**
What is the difference between the two wildcards ... and * for the monitor stanza in inputs.conf?

A. ... is not supported in monitor stanzas.
B. There is no difference, they are interchangeable and match anything beyond directory boundaries.
C. * matches anything in that specific directory path segment, whereas ... recurses through subdirectories as well.
D. ... matches anything in that specific directory path segment, whereas * recurses through subdirectories as well.

**Answer:** C

**Explanation:**
Reference: https://docs.splunk.com/Documentation/Splunk/7.3.0/Data/Specifyinputpathswithwildcards

**NEW QUESTION 34**
What type of data is counted against the Enterprise license at a fixed 150 bytes per event?

A. License data
B. Metrics data
C. Internal Splunk data
D. Internal Windows logs

**Answer:** B

**Explanation:**
Reference: https://answers.splunk.com/answers/581441/how-is-the-splunk-license-measured.html

**NEW QUESTION 38**
Where are license files stored?

A. $SPLUNK_HOME/etc/secure
B. $SPLUNK_HOME/etc/system
C. $SPLUNK_HOME/etc/licenses
D. $SPLUNK_HOME/etc/apps/licenses

**Answer:** C

**Explanation:**
Reference: https://docs.splunk.com/Documentation/Splunk/7.3.1/Admin/LicenserCLIcommands

**NEW QUESTION 43**
In this sourcetype definition the MAX_TIMESTAMP_LOOKAHEAD is missing. Which value would fit best?
[sshd_syslog] TIME_PREFIX = ^
TIME_FORMAT = %Y-%m-%d %H:%M:%S.%3N %z
LINE_BREAKER = ([\r\n]+)\d{4}-\d{2}-\d{2} \d{2}:\d{2}:\d{2} SHOUD_LINEMERGE = false
TRUNCATE = 0
Event example: 2018-04-13 13:42:41.214 -0500 server sshd[26219]: Connection from 172.0.2.60 port 47366

A. MAX_TIMESTAMP_LOOKAHEAD = 5
B. MAX_TIMESTAMP_LOOKAHEAD = 10
C. MAX_TIMESTAMP_LOOKAHEAD = 20
D. MAX_TIMESTAMP_LOOKAHEAD = 30

**Answer:** B

**NEW QUESTION 46**
.....

# THANKS FOR TRYING THE DEMO OF OUR PRODUCT

Visit Our Site to Purchase the Full Set of Actual SPLK-1003 Exam Questions With Answers.

We Also Provide Practice Exam Software That Simulates Real Exam Environment And Has Many Self-Assessment Features. Order the SPLK-1003 Product From:

**https://www.2passeasy.com/dumps/SPLK-1003/**

## Money Back Guarantee

**SPLK-1003 Practice Exam Features:**

* SPLK-1003 Questions and Answers Updated Frequently

* SPLK-1003 Practice Questions Verified by Expert Senior Certified Staff

* SPLK-1003 Most Realistic Questions that Guarantee you a Pass on Your FirstTry

* SPLK-1003 Practice Test Questions in Multiple Choice Formats and Updatesfor 1 Year