

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 case of a conflict between a whitelist and a blacklist input setting, which one is used?

- A. Blacklist
- B. Whitelist
- C. They cancel each other out.
- D. Whichever is entered into the configuration first.

Answer: A

Explanation:

Reference: <https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=8&ved=2ahUKEwj0r6Lso6bkAhUqxYUKHbWIDz4QFjAHegQIAxAC&url=http%3A%2F%2Fsplunk.training%2Fshowpdf.asp%3Fdata%3D789BB6B10C1B4376B548D711B4377F3F4B511B437805A8EC11B437742EA8F11B43779B6FA211B4376EA657C11B4376FC19B311B4377E2407E11B43730AF97411B4377F3F4B511B437742EA8F11B43779B6FA211B43771F822111B437731365811B43730AF97411B437789BB6B11B4376B548D711B4377F3F4B511B437805A8EC11B437742EA8F11B43779B6FA211B4376EA657C11B4376FC19B311B4377E2407E11B43732E61E211B4377F3F4B511B437742EA8F11B43779B6FA211B43771F822111B437731365811B43746D0DC011B4377549EC611B4377BED81011B437789BB6B11B4376D8B14511B437731365811B4376B548D711B4377F3F4B511B4376FC19B311B43732E61E211B4376D8B14511B4377AD23D911B437789BB6B11B43730AF97411B4373989B2C11B437386E6F511B437386E6F511B4373DF6C0811B43737532BE11B4373BC039A11B437351CA5011B43737532BE11B43730AF97411B4375BD6DD511B43730AF97411B437564E8C211B43730AF97411B437%257C2318D1%257C11649A&usg=AOvVaw2e9s-JweivuCkqTb4-Y9uW>

NEW QUESTION 3

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 4

Which of the following are supported configuration methods to add inputs on a forwarder? (Select all that apply.)

- A. CLI
- B. Edit inputs.conf
- C. Edit forwarder.conf
- D. Forwarder Management

Answer: B

Explanation:

Reference: <https://docs.splunk.com/Documentation/Forwarder/7.3.1/Forwarder/Configuretheuniversalforwarder>

NEW QUESTION 5

Which parent directory contains the configuration files in Splunk?

- A. \$SPLUNK_HOME/etc
- B. \$SPLUNK_HOME/var
- C. \$SPLUNK_HOME/conf
- D. \$SPLUNK_HOME/default

Answer: A

Explanation:

Reference: <https://docs.splunk.com/Documentation/Splunk/7.3.1/Admin/Configurationfiledirectories>

NEW QUESTION 6

Which forwarder type can parse data prior to forwarding?

- A. Universal forwarder
- B. Heaviest forwarder
- C. Hyper forwarder
- D. Heavy forwarder

Answer: D

Explanation:

Reference: <https://docs.splunk.com/Documentation/Splunk/7.3.1/Forwarding/Typesofforwarders>

NEW QUESTION 7

Which Splunk component consolidates the individual results and prepares reports in a distributed environment?

- A. Indexers
- B. Forwarder
- C. Search head
- D. Search peers

Answer: A

Explanation:

Reference: <https://docs.splunk.com/Documentation/Splunk/7.3.1/Indexer/Advancedindexingstrategy>

NEW QUESTION 8

Which Splunk component distributes apps and certain other configuration updates to search head cluster members?

- A. Deployer
- B. Cluster master
- C. Deployment server
- D. Search head cluster master

Answer: A

Explanation:

Reference: <https://docs.splunk.com/Documentation/Splunk/7.3.1/DistSearch/PropagateSHCconfigurationchanges>

NEW QUESTION 9

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 10

This file has been manually created on a universal forwarder:

```
/opt/splunkforwarder/etc/apps/my_TA/local/inputs.conf [monitor:///var/log/messages]
```

```
sourcetype=syslog
```

```
index=syslog
```

A new Splunk admin comes in and connects the universal forwarders to a deployment server and deploys the same app with a new inputs.conf file:

```
/opt/splunk/etc/deployment-apps/my_TA/local/inputs.conf
```

```
[monitor:///var/log/maillog] sourcetype=maillog index=syslog
```

Which file is now monitored?

- A. /var/log/messages
- B. /var/log/maillog
- C. /var/log/maillog and /var/log/messages
- D. none of the above

Answer: C

NEW QUESTION 10

In which phase of the index time process does the license metering occur?

- A. Input phase
- B. Parsing phase
- C. Indexing phase
- D. Licensing phase

Answer: C

Explanation:

Reference: <https://docs.splunk.com/Documentation/Splunk/7.3.1/Admin/HowSplunklicensingworks>

NEW QUESTION 12

You update a props.conf file while Splunk is running. You do not restart Splunk and you run this command: splunk btool props list —debug. What will the output be?

- A. A list of all the configurations on-disk that Splunk contains.
- B. A verbose list of all configurations as they were when splunkd started.
- C. A list of props.conf configurations as they are on-disk along with a file path from which the configuration is located.
- D. A list of the current running props.conf configurations along with a file path from which the configuration was made.

Answer: D

Explanation:

Reference: <https://answers.splunk.com/answers/494219/need-help-with-what-should-be-a-simple-precedence.html>

NEW QUESTION 17

What is required when adding a native user to Splunk? (Select all that apply.)

- A. Password
- B. Username
- C. Full Name
- D. Default app

Answer: CD

Explanation:

Reference: <https://docs.splunk.com/Documentation/Splunk/7.3.1/Security/Addandeditusers>

NEW QUESTION 21

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 25

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 30

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 35

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 40

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/Configurecharacterencoding>

NEW QUESTION 45

Which of the following enables compression for universal forwarders in outputs.conf?

- A. [udpout:mysplunk_indexer11] compression=true
- B. [tcpout] defaultGroup=my_indexers compressed=true
- C. /opt/splunkforwarder/bin/splunk enable compression
- D. [tcpout:my_indexers] server=mysplunk_indexer1:9997, mysplunk_indexer2:9997 decompression=false

Answer: B

Explanation:

Reference: <https://docs.splunk.com/Documentation/Splunk/7.3.1/Admin/Outputsconf>

NEW QUESTION 48

User role inheritance allows what to be inherited from the parent role? (Select all that apply.)

- A. Parents
- B. Capabilities
- C. Index access
- D. Search history

Answer: B

Explanation:

Reference: https://docs.splunk.com/Documentation/Splunk/7.3.1/Security/Aboutusersandroles#How_users_inherit_capabilities

NEW QUESTION 51

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 54

How do you remove missing forwarders from the Monitoring Console?

- A. By restarting Splunk.
- B. By rescanning active forwarders.
- C. By reloading the deployment server.
- D. By rebuilding the forwarder asset table.

Answer: D

Explanation:

Reference: <https://answers.splunk.com/answers/447096/how-to-remove-missing-forwarders-from-the-distribu.html>

NEW QUESTION 59

How often does Splunk recheck the LDAP server?

- A. Every 5 minutes.
- B. Each time a user logs in.
- C. Each time Splunk is restarted.
- D. Varies based on LDAP_refresh setting.

Answer: D

Explanation:

Reference: <http://docshare02.docshare.tips/files/22651/226514302.pdf>

NEW QUESTION 64

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 66

Which Splunk component performs indexing and responds to search requests from the search head?

- A. Forwarder
- B. Search peer
- C. License master
- D. Search head cluster

Answer: B

Explanation:

Reference: <https://www.edureka.co/blog/splunk-architecture/>

NEW QUESTION 69

When deploying apps, which attribute in the forwarder management interface determines the apps that clients install?

- A. App Class
- B. Client Class
- C. Server Class
- D. Forwarder Class

Answer: C

Explanation:

Reference: <https://docs.splunk.com/Documentation/Splunk/7.3.1/Updating/Createdeploymentapps>

NEW QUESTION 72

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 75

.....

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