

Splunk

Exam Questions SPLK-1003

Splunk Enterprise Certified Admin



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

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 4

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 5

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 6

What are the minimum required settings when creating a network input in Splunk?

- A. Protocol, port number
- B. Protocol, port, location
- C. Protocol, username, port
- D. Protocol, IP, port number

Answer: A

Explanation:

Reference: <https://docs.splunk.com/Documentation/Splunk/7.3.1/Data/UsetheHTTPEventCollector>

NEW QUESTION 7

Which Splunk component requires a Forwarder license?

- A. Search head
- B. Heavy forwarder
- C. Heaviest forwarder
- D. Universal forwarder

Answer: B

Explanation:

Reference: <https://answers.splunk.com/answers/70017/heavy-forwarder-costs-and-licenses.html>

NEW QUESTION 8

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 9

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 10

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 10

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 12

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 13

How would you configure your distsearch.conf to allow you to run the search below?

```
sourcetype=access_combined status=200 action=purchase splunk_server_group=HOUSTON
```

- A. [distributedSearch:NYC] default = false servers = nyc1:8089, nyc2:8089 [distributedSearch:HOUSTON] default = false servers = houston1:8089, houston2:8089
- B. [distributedSearch] servers =nyc1, nyc2, houston1, houston2 [distributedSearch:NYC] default = false servers = nyc1, nyc2 [distributedSearch:HOUSTON]default = false servers = houston1, houston2
- C. [distributedSearch] servers =nyc1:8089, nyc2:8089, houston1:8089, houston2:8089[distributedSearch:NYC] default= false servers = nyc1:8089, nyc2:8089 [distributedSearch:HOUSTON]default = false servers = houston1:8089, houston2:8089
- D. [distributedSearch] servers =nyc1:8089; nyc2:8089; houston1:8089; houston2:8089[distributedSearch:NYC]default = false servers = nyc1:8089; nyc2:8089 [distributedSearch:HOUSTON] default = false servers = houston1:8089; houston2:8089

Answer: D

NEW QUESTION 14

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 16

Which of the following are methods for adding inputs in Splunk? (Select all that apply.)

- A. CLI
- B. Splunk Web
- C. Editing inpits.conf
- D. Editing monitor.conf

Answer: AB

Explanation:

Reference: <http://dev.splunk.com/view/dev -guide/SP-CAAAE3A>

NEW QUESTION 19

Which Splunk indexer operating system platform is supported when sending logs from a Windows universal forwarder?

- A. Any OS platform.
- B. Linux platform only.
- C. Windows platform only.
- D. None of the above.

Answer: C

NEW QUESTION 24

What are the required stanza attributes when configuring the transforms.conf to manipulate or remove events?

- A. REGEX, DEST, FORMAT
- B. REGEX, SRC_KEY, FORMAT
- C. REGEX, DEST_KEY, FORMAT
- D. REGEX, DEST_KEY, FORMATTING

Answer: C

Explanation:

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

NEW QUESTION 28

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} SHOULD_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 30

Which of the following apply to how distributed search works? (Select all that apply.)

- A. The search head dispatches searches to the peers.
- B. The search peers pull the data from the forwarders.
- C. Peers run searches in parallel and return their portion of results.
- D. The search head consolidates the individual results and prepares reports.

Answer: A

Explanation:

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

NEW QUESTION 32

With authentication methods are natively supported within Splunk Enterprise? (Select all that apply.)

- A. LDAP
- B. SAML
- C. RADIUS
- D. Duo Multifactor Authentication

Answer: AD

Explanation:

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

NEW QUESTION 36

.....

Thank You for Trying Our Product

We offer two products:

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

2nd - Questions and Answers in PDF Format

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

100% Actual & Verified — Instant Download, Please Click
[Order The SPLK-1003 Practice Test Here](#)