



# Splunk

## Exam Questions SPLK-1003

Splunk Enterprise Certified Admin

#### NEW QUESTION 1

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 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

The priority of layered Splunk configuration files depends on the file's:

- A. Owner
- B. Weight
- C. Context
- D. Creation time

**Answer:** C

#### Explanation:

Reference: <https://docs.splunk.com/Documentation/Splunk/7.3.0/Admin/Wheretofindtheconfigurationfiles>

#### NEW QUESTION 4

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/Adddandeditusers>

#### NEW QUESTION 5

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 6

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 7

Which of the following statements apply to directory inputs? (Select all that apply.)

- A. All discovered text files are consumed.  
B. Compressed files are ignored by default.  
C. Splunk recursively traverses through the directory structure.  
D. When adding new log files to a monitored directory, the forwarder must be restarted to take them into account.

**Answer:** C

**Explanation:**

Reference: <https://answers.splunk.com/answers/133875/recursive-monitoring-of-directories.html>

#### NEW QUESTION 8

Which Splunk component does a search head primarily communicate with?

- A. Indexer  
B. Forwarder  
C. Cluster master  
D. Deployment server

**Answer:** A

**Explanation:**

Reference: <https://docs.splunk.com/Documentation/Splunk/7.3.1/InheritedDeployment/Deploymenttopology>

#### NEW QUESTION 9

Which layers are involved in Splunk configuration file layering? (Select all that apply.)

- A. App context  
B. User context  
C. Global context  
D. Forwarder context

**Answer:** AC

**Explanation:**

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

#### NEW QUESTION 10

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 10

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 12

Which of the following indexes come pre-configured with Splunk Enterprise? (Select all that apply.)

- A. \_licence
- B. \_internal
- C. \_external
- D. \_thefishbucket

**Answer:** B

**Explanation:**

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

#### NEW QUESTION 13

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 18

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 19

.....

## About ExamBible

*[Your Partner of IT Exam](#)*

## Found in 1998

ExamBible is a company specialized on providing high quality IT exam practice study materials, especially Cisco CCNA, CCDA, CCNP, CCIE, Checkpoint CCSE, CompTIA A+, Network+ certification practice exams and so on. We guarantee that the candidates will not only pass any IT exam at the first attempt but also get profound understanding about the certificates they have got. There are so many alike companies in this industry, however, ExamBible has its unique advantages that other companies could not achieve.

## Our Advances

### \* 99.9% Uptime

All examinations will be up to date.

### \* 24/7 Quality Support

We will provide service round the clock.

### \* 100% Pass Rate

Our guarantee that you will pass the exam.

### \* Unique Gurantee

If you do not pass the exam at the first time, we will not only arrange FULL REFUND for you, but also provide you another exam of your claim, ABSOLUTELY FREE!

#### NEW QUESTION 1

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 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

The priority of layered Splunk configuration files depends on the file's:

- A. Owner
- B. Weight
- C. Context
- D. Creation time

**Answer:** C

#### Explanation:

Reference: <https://docs.splunk.com/Documentation/Splunk/7.3.0/Admin/Wheretofindtheconfigurationfiles>

#### NEW QUESTION 4

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/Adddandeditusers>

#### NEW QUESTION 5

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 6

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 7

Which of the following statements apply to directory inputs? (Select all that apply.)

- A. All discovered text files are consumed.  
B. Compressed files are ignored by default.  
C. Splunk recursively traverses through the directory structure.  
D. When adding new log files to a monitored directory, the forwarder must be restarted to take them into account.

**Answer:** C

**Explanation:**

Reference: <https://answers.splunk.com/answers/133875/recursive-monitoring-of-directories.html>

#### NEW QUESTION 8

Which Splunk component does a search head primarily communicate with?

- A. Indexer  
B. Forwarder  
C. Cluster master  
D. Deployment server

**Answer:** A

**Explanation:**

Reference: <https://docs.splunk.com/Documentation/Splunk/7.3.1/InheritedDeployment/Deploymenttopology>

#### NEW QUESTION 9

Which layers are involved in Splunk configuration file layering? (Select all that apply.)

- A. App context  
B. User context  
C. Global context  
D. Forwarder context

**Answer:** AC

**Explanation:**

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

#### NEW QUESTION 10

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 10

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 12

Which of the following indexes come pre-configured with Splunk Enterprise? (Select all that apply.)

- A. \_licence
- B. \_internal
- C. \_external
- D. \_thefishbucket

**Answer:** B

**Explanation:**

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

#### NEW QUESTION 13

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 18

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 19

.....



## Relate Links

**100% Pass Your SPLK-1003 Exam with ExamBible Prep Materials**

<https://www.exambible.com/SPLK-1003-exam/>

## Contact us

We are proud of our high-quality customer service, which serves you around the clock 24/7.

Viste - <https://www.exambible.com/>