DUMPSBOSS.

Splunk Enterprise Certified Admin

Splunk SPLK-1003

Version Demo

Total Demo Questions: 10

Total Premium Questions: 137

Buy Premium PDF

https://dumpsboss.co

support@dumpsboss.co

support@dumpsboss.co
dumpsboss.co

QUESTION NO: 1

Which of the following configuration files are used with a universal forwarder? (Choose all that apply.)

A. inputs.conf

B. monitor.conf

C. outputs.conf

D. forwarder.conf

ANSWER: A C

Explanation:

Reference: https://docs.splunk.com/Documentation/Forwarder/8.0.5/Forwarder/Configuretheuniversalforwarder

QUESTION NO: 2

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

ANSWER: C

Explanation:

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

QUESTION NO: 3

In which phase do indexed extractions in props.conf occur?

A. Inputs phase

B. Parsing phase

C. Indexing phase

D. Searching phase

ANSWER: B

Explanation:

Reference: https://docs.splunk.com/Documentation/Splunk/8.0.5/Admin/Configurationparametersandthedatapipeline

QUESTION NO: 4

Which network input option provides durable file-system buffering of data to mitigate data loss due to network outages and splunkd restarts?

A. diskQueueSize

B. durableQueueSize

C. persistentQueueSize

D. queueSize

ANSWER: C

Explanation:

Reference: https://docs.splunk.com/Documentation/SplunkCloud/8.2.2111/Data/Usepersistentqueues

QUESTION NO: 5

Which of the following Splunk components require a separate installation package?

A. Deployment server

B. License master

C. Universal forwarder

D. Heavy forwarder

ANSWER: C

Explanation:

Reference: https://github.com/packetiq/SplunkArchitect/blob/master/Install-and-Configure-Splunk-Enterprise-Components.md

QUESTION NO: 6

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

A. Password

B. Username

C. Full Name

D. Default app

ANSWER: C D

Explanation:

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

QUESTION NO: 7

What happens when the same username exists in Splunk as well as through LDAP?

A. Splunk user is automatically deleted from authentication.conf.

B. LDAP settings take precedence.

C. Splunk settings take precedence.

D. LDAP user is automatically deleted from authentication.conf.

ANSWER: C

Explanation:

Reference: https://docs.splunk.com/Documentation/SplunkCloud/8.2.2105/Security/SetupuserauthenticationwithLDAP

Following are the main steps to configure the Splunk platform to work with LDAP for authentication:

1. Configure one or more LDAP strategies, typically one strategy per LDAP server.
2. Map LDAP groups to one or more Splunk roles.
3. If you have multiple LDAP servers, specify the connection order of the servers.

In Splunk Cloud, you can perform these steps in Splunk Web. See Configure LDAP with Splunk Web.

In Splunk Enterprise, you can use either Splunk Web or configuration files to configure LDAP. To use configuration files to configure LDAP, see Configure LDAP with configuration files.

QUESTION NO: 8

An index stores its data in buckets. Which default directories does Splunk use to store buckets? (Choose all that apply.)

A. bucketdb

B. frozendb

C. colddb

D. db

ANSWER: B C

Explanation:

Reference: https://docs.splunk.com/Documentation/Splunk/8.2.1/Indexer/Bucketsandclusters

QUESTION NO: 9

Which valid bucket types are searchable? (Choose all that apply.)

A. Hot buckets

B. Cold buckets

C. Warm buckets

D. Frozen buckets

ANSWER: A B C

Explanation:

Reference: https://docs.splunk.com/Documentation/Splunk/7.3.1/Indexer/HowSplunkstoresindexes

QUESTION NO: 10

Within props.conf, which stanzas are valid for data modification? (Choose all that apply.)

A. Host

B. Server

C. Source

D. Sourcetype

ANSWER: C D

Explanation:

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