SPLK-1003 Q&As

Splunk Enterprise Certified Admin

Pass Splunk SPLK-1003 Exam with 100% Guarantee

Free Download Real Questions & Answers **PDF** and **VCE** file from:

https://www.passapply.com/splk-1003.html

100% Passing Guarantee
100% Money Back Assurance

Following Questions and Answers are all new published by Splunk Official Exam Center

- **Instant Download** After Purchase
- **100% Money Back** Guarantee
- **365 Days** Free Update
- **800,000+** Satisfied Customers

QUESTION 1

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.

Correct Answer: AB

https://docs.splunk.com/Documentation/Splunk/8.2.2/Admin/Distdeploylicenses#:~:text=License%20requirements,do%20not%20index%20external%20data.

"All Splunk Enterprise instances functioning as management components needs access to an Enterprise license. Management components include the deployment server, the indexer cluster manager node, the search head cluster deployer, and the monitoring console."

https://docs.splunk.com/Documentation/Splunk/8.2.2/Updating/Aboutdeploymentserver

"The deployment server is the tool for distributing configurations, apps, and content updates to groups of Splunk Enterprise instances."

QUESTION 2

Who provides the Application Secret, Integration, and Secret keys, as well as the API Hostname when setting up Duo for Multi-Factor Authentication in Splunk Enterprise?

A. Duo Administrator

B. LDAP Administrator

C. SAML Administrator

D. Trio Administrator

Correct Answer: A

Reference: https://duo.com/docs/splunk

QUESTION 3

Which setting allows the configuration of Splunk to allow events to span over more than one line?

A. SHOULD_LINEMERGE = true

B. BREAK_ONLY_BEFORE_DATE = true

C. BREAK_ONLY_BEFORE =

D. SHOULD_LINEMERGE = false

Correct Answer: C

Reference: https://docs.splunk.com/Documentation/SplunkCloud/latest/Data/Configureeventlinebreaking

QUESTION 4

In a distributed environment, which Splunk component is used to distribute apps and configurations to the other Splunk instances?

A. Indexer

B. Deployer

C. Forwarder

D. Deployment server

Correct Answer: D

Reference: https://docs.splunk.com/Documentation/Splunk/8.0.5/Updating/Updateconfigurations

QUESTION 5

When are knowledge bundles distributed to search peers?

A. After a user logs in.

B. When Splunk is restarted.

C. When adding a new search peer.

D. When a distributed search is initiated.

Correct Answer: D

"The search head replicates the knowledge bundle periodically in the background or when initiating a search. " "As part of the distributed search process, the search head replicates and distributes its knowledge objects to its search peers, or indexers. Knowledge objects include saved searches, event types, and other entities used in searching accorss indexes. The search head needs to distribute this material to its search peers so that they can properly execute queries on its behalf."

Reference: https://docs.splunk.com/Documentation/Splunk/8.0.5/DistSearch/Whatsearchheadssend