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.pass2lead.com/splk-1003.html

100% Passing Guarantee
100% Money Back Assurance

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

QUESTION 1

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 2

What action is required to enable forwarder management in Splunk Web?

A. Navigate to Settings > Server Settings > General Settings, and set an App server port.

B. Navigate to Settings > Forwarding and receiving, and click on Enable Forwarding.

C. Create a server class and map it to a client in SPLUNK_HOME/etc/system/local/serverclass.conf.

D. Place an app in the SPLUNK_HOME/etc/deployment-apps directory of the deployment server.

Correct Answer: C

To activate deployment server, you must place at least one app into %SPLUNK_HOME%\etc\deployment-apps on the host you want to act as deployment server. In this case, the app is the "send to indexer" app you created earlier, and the host is the indexer you set up initially. Reference:
https://docs.splunk.com/Documentation/Splunk/8.2.1/Updating/Forwardermanagementoverview
https://docs.splunk.com/Documentation/MSApp/2.0.3/MSInfra/Setupadeploymentserver

QUESTION 3

When using a directory monitor input, specific source type can be selectively overridden using which configuration file?

A. props.conf

B. sourcetypes.conf

C. transforms.conf

D. outputs.conf

Correct Answer: A

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

QUESTION 4

When running a real-time search, search results are pulled from which Splunk component?

A. Heavy forwarders and seach peers

B. Heavy forwarders

C. Search heads

D. Search peers

Correct Answer: D

Using the Splunk reference URL https://docs.splunk.com/Splexicon:Searchpeer

"search peer is a splunk platform instance that responds to search requests from a search head. The term "search peer" is usally synonymous with the indexer role in a distributed search topology. However, other instance types also have access to indexed data, particularly internal diagnostic data, and thus function as search peers when they respond to search requests for that data."

QUESTION 5

How is data handled by Splunk during the input phase of the data ingestion process?

A. Data is treated as streams.

B. Data is broken up into events.

C. Data is initially written to disk.

D. Data is measured by the license meter.

Correct Answer: A

In the input segment, Splunk software consumes data. It acquires the raw data stream from its source, breaks in into 64K blocks, and annotates each block with some metadata keys.

Reference: https://docs.splunk.com/Documentation/Splunk/8.0.5/Deploy/Datapipeline