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.geekcert.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

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 2

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

Correct Answer: BD

https://docs.splunk.com/Documentation/Splunk/8.0.1/Forwarding/Aboutforwardingandreceivingdat a

---

QUESTION 3

Which of the following are available input methods when adding a file input in Splunk Web? (Choose all that apply.)

A. Index once.

B. Monitor interval.

C. On-demand monitor.

D. Continuously monitor.

Correct Answer: AD

https://docs.splunk.com/Documentation/Splunk/8.2.2/Data/Howdoyouwanttoadddata

The fastest way to add data to your Splunk Cloud instance or Splunk Enterprise deployment is to use Splunk Web. After you access the Add Data page, choose one of three options for getting data into your Splunk platform deployment with Splunk Web: (1) Upload, (2) Monitor, (3) Forward The Upload option lets you upload a file or archive of files for indexing. When you choose Upload option, Splunk Web opens the upload process page. Monitor. For Splunk Enterprise installations, the Monitor option lets you monitor one or more files, directories, network streams, scripts, Event Logs (on Windows hosts only), performance metrics, or any other type of machine data that the Splunk Enterprise instance has access to.

QUESTION 4

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

Correct Answer: A

https://docs.splunk.com/Documentation/Splunk/8.0.5/Admin/Inputsconf

[tcp://:]

*Configures the input to listen on a specific TCP network port. *If a makes a connection to this instance, the input uses this stanza to configure itself.

*If you do not specify , this stanza matches all connections on the specified port.

*Generates events with source set to "tcp:", for example: tcp:514 *If you do not specify a sourcetype, generates events with sourcetype set to "tcp-raw"

QUESTION 5

Using SEDCMD in props.conf allows raw data to be modified. With the given event below, which option will mask the first three digits of the AcctID field resulting output: [22/Oct/2018:15:50:21] VendorID=1234 Code=B AcctID=xxx5309

Event:

[22/Oct/2018:15:50:21] VendorID=1234 Code=B AcctID=xxx5309

A. SEDCMD-1acct = s/VendorID=\d{3}(\d{4})/VendorID=xxx/g

B. SEDCMD-xxxAcct = s/AcctID=\d{3}(\d{4})/AcctID=xxx/g

C. SEDCMD-1acct = s/AcctID=\d{3}(\d{4})/AcctID=\1xxx/g

D. SEDCMD-1acct = s/AcctID=\d{3}(\d{4})/AcctID=xxx\1/g

Correct Answer: D

Latest SPLK-1003 Dumps SPLK-1003 Study Guide SPLK-1003 Exam Questions