SPLK-1003$^{\text{Q\&As}}$

Splunk Enterprise Certified Admin

QUESTION 1

A new forwarder has been installed with a manually createddeploymentclient.conf.

What is the next step to enable the communication between the forwarder and the deployment server?

A. Restart Splunk on the deployment server.

B. Enable the deployment client in Splunk Web under Forwarder Management.

C. Restart Splunk on the deployment client.

D. Wait for up to the time set in thephoneHomeIntervalInSecssetting.

Correct Answer: C

The next step to enable the communication between the forwarder and the deployment server after installing a new forwarder with a manually created deploymentclient.conf is to restart Splunk on the deployment client. The deploymentclient.conf file contains the settings for the deployment client, which is a Splunk instance that receives updates from the deployment server. The file must include the targetUri attribute, which specifies the hostname and management port of the deployment server. To apply the changes in the deploymentclient.conf file, Splunk must be restarted on the deployment client. Therefore, option C is the correct answer. References: Splunk Enterprise Certified Admin | Splunk, [Configure deployment clients - Splunk Documentation]

QUESTION 2

How does the Monitoring Console monitor forwarders?

A. By pulling internal logs from forwarders.

B. By using the forwarder monitoring add-on

C. With internal logs forwarded by forwarders.

D. With internal logs forwarded by deployment server.

Correct Answer: C

Quoting the following Splunk URL reference https://docs.splunk.com/Documentation/Splunk/8.2.2/DMC/DMCprerequisites "Monitoring Console setup prerequisites. Forward internal logs (both $SPLUNK_HOME/car/log/splunk and$SPLUNK_HOME/var/log/introspection) to indexers from all other components. Without this step, many dashboards will lack data."

QUESTION 3

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

Correct Answer: C

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

Splunk platform attempts native authentication first. If authentication fails outside of a local account that doesn\\'t exist, there is no attempt to use LDAP to log in. This is adapted from precedence of Splunk authentication schema.

QUESTION 4

A log file contains 193 days worth of timestamped events. Which monitor stanza would be used to collect data 45 days old and newer from that log file?

A. followTail = -45d

B. ignore = 45d

C. includeNewerThan = -35d

D. ignoreOlderThan = 45d

Correct Answer: D

Reference:https://docs.splunk.com/Documentation/Splunk/8.2.1/Data/Configuretimestampr ecognition

QUESTION 5

During search time, which directory of configuration files has the highest precedence?

A. $SFLUNK_KOME/etc/system/local

B. $SPLUNK_KCME/etc/system/default

C. $SPLUNK_HCME/etc/apps/app1/local

D. $SPLUNK HCME/etc/users/admin/local

Correct Answer: D

Adding further clarity and quoting same Splunk reference URL from @giubal"

"To keep configuration settings consistent across peer nodes, configuration files are managed from the cluster master, which pushes the files to the slave-app directories on the peer nodes. Files in the slave-app directories have the highest precedence in a cluster peer\\'s configuration. Here is the expanded precedence order for cluster peers: 1.Slave-app local directories -- highest priority

2.

System local directory

3.

App local directories

4.

Slave-app default directories

5.

App default directories

6.

System default directory --lowest priority