Splunk

Exam Questions SPLK-1003

Splunk Enterprise Certified Admin

NEW QUESTION 1
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

Answer: D

Explanation:
Reference: https://docs.splunk.com/Documentation/Splunk/7.3.1/Forwarding/Typesofforwarders

NEW QUESTION 2
Which of the following are supported configuration methods to add inputs on a forwarder? (Select all that apply.)

A. CLI
B. Edit inputs.conf
C. Edit forwarder.conf
D. Forwarder Management

Answer: B

Explanation:
Reference: https://docs.splunk.com/Documentation/Forwarder/7.3.1/Forwarder/Configuretheuniversalforwarder

NEW QUESTION 3
Which parent directory contains the configuration files in Splunk?

A. $SPLUNK_HOME/etc
B. $SPLUNK_HOME/var
C. $SPLUNK_HOME/conf
D. $SPLUNK_HOME/default

Answer: A

Explanation:
Reference: https://docs.splunk.com/Documentation/Splunk/7.3.1/Admin/Configurationfiledirectories

NEW QUESTION 4
Which Splunk component distributes apps and certain other configuration updates to search head cluster members?

A. Deployer
B. Cluster master
C. Deployment server
D. Search head cluster master

Answer: A

Explanation:
Reference: https://docs.splunk.com/Documentation/Splunk/7.3.1/DistSearch/PropagateSHCconfigurationchanges

NEW QUESTION 5
Where should apps be located on the deployment server that the clients pull from?

A. $SPLUNK_HOME/etc/apps
B. $SPLUNK_HOME/etc/search
C. $SPLUNK_HOME/etc/master-apps
D. $SPLUNK_HOME/etc/deployment-apps

Answer: A

Explanation:
Reference: https://answers.splunk.com/answers/371099/how-to-configure-deployment-apps-to-push-to-client.html

NEW QUESTION 6
This file has been manually created on a universal forwarder:
/opt/splunkforwarder/etc/apps/my_TA/local/inputs.conf [monitor:///var/log/messages]
sourcetype=syslog
index=syslog
A new Splunk admin comes in and connects the universal forwarders to a deployment server and deploys the same app with a new inputs.conf file:
/opt/splunk/etc/deployment-apps/my_TA/local/inputs.conf
[monitor:///var/log/maillog] sourcetype=maillog index=syslog
Which file is now monitored?

A. /var/log/messages
B. /var/log/maillog
C. /var/log/maillog and /var/log/messages
D. none of the above

Answer: C

NEW QUESTION 7
When running the command shown below, what is the default path in which deploymentserver.conf is created?
splunk set deploy-poll deployServer:port

A. SPLUNK_HOME/etc/deployment
B. SPLUNK_HOME/etc/system/local
C. SPLUNK_HOME/etc/system/default
D. SPLUNK_HOME/etc/apps/deployment

Answer: B

Explanation:
Reference: https://docs.splunk.com/Documentation/Splunk/7.3.1/Updating/Configuredeploymentclients

NEW QUESTION 8
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

Answer: A

Explanation:
Reference: https://docs.splunk.com/Documentation/Splunk/7.3.1/Data/UsetheHTTPEventCollector

NEW QUESTION 9
Which Splunk component requires a Forwarder license?

A. Search head
B. Heavy forwarder
C. Heaviest forwarder
D. Universal forwarder

Answer: B

Explanation:
Reference: https://answers.splunk.com/answers/70017/heavy-forwarder-costs-and-licenses.html

NEW QUESTION 10
Which optional configuration setting in inputs.conf allows you to selectively forward the data to specific indexer(s)?

A. _TCP_ROUTING
B. _INDEXER_LIST
C. _INDEXER_GROUP
D. _INDEXER_ROUTING

Answer: A

Explanation:
Reference: https://docs.splunk.com/Documentation/Splunk/7.3.1/Data/Monitorfilesanddirectorieswithinputs.conf

NEW QUESTION 10
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.

Answer: A

NEW QUESTION 13
During search time, which directory of configuration files has the highest precedence?

A. $SPLUNK_HOME/etc/system/local
B. $SPLUNK_HOME/etc/system/default
C. $SPLUNK_HOME/etc/apps/app1/local

D. $SPLUNK_HOME/etc/users/admin/local

Answer: C

Explanation:
Reference: https://docs.splunk.com/Documentation/Splunk/7.3.0/Admin/Wheretofindtheconfigurationfiles

NEW QUESTION 17
User role inheritance allows what to be inherited from the parent role? (Select all that apply.)

A. Parents
B. Capabilities
C. Index access
D. Search history

Answer: B

Explanation:
Reference: https://docs.splunk.com/Documentation/Splunk/7.3.1/Security/Aboutusersandroles#How_users_inherit_capabilities

NEW QUESTION 18
Which of the following statements apply to directory inputs? (Select all that apply.)

A. All discovered text files are consumed.
B. Compressed files are ignored by default.
C. Splunk recursively traverses through the directory structure.
D. When adding new log files to a monitored directory, the forwarder must be restarted to take them into account.

Answer: C

Explanation:
Reference: https://answers.splunk.com/answers/133875/recursive-monitoring-of -directories.html

NEW QUESTION 22
Local user accounts created in Splunk store passwords in which file?

A. $SPLUNK_HOME/etc/passwd
B. $SPLUNK_HOME/etc/authentication
C. $SPLUNK_HOME/etc/users/passwd.conf
D. $SPLUNK_HOME/etc/users/authentication.conf

Answer: A

Explanation:
Reference: https://docs.splunk.com/Documentation/Splunk/7.3.1/Admin/User-seedconf

NEW QUESTION 25
What is the difference between the two wildcards ... and * for the monitor stanza in inputs.conf?

A. ... is not supported in monitor stanzas.
B. There is no difference, they are interchangeable and match anything beyond directory boundaries.
C. * matches anything in that specific directory path segment, whereas ... recurses through subdirectories as well.
D. ... matches anything in that specific directory path segment, whereas * recurses through subdirectories as well.

Answer: C

Explanation:
Reference: https://docs.splunk.com/Documentation/Splunk/7.3.0/Data/Specifyinputpathswithwildcards

NEW QUESTION 28
How do you remove missing forwarders from the Monitoring Console?

A. By restarting Splunk.
B. By rescanning active forwarders.
C. By reloading the deployment server.
D. By rebuilding the forwarder asset table.

Answer: D

Explanation:
Reference: https://answers.splunk.com/answers/447096/how-to-remove-missing-forwarders-from-the-distribu.html

NEW QUESTION 30
Which Splunk indexer operating system platform is supported when sending logs from a Windows universal forwarder?

A. Any OS platform.

B. Linux platform only.
C. Windows platform only.
D. None of the above.

Answer: C

NEW QUESTION 34
How often does Splunk recheck the LDAP server?

A. Every 5 minutes.
B. Each time a user logs in.
C. Each time Splunk is restarted.
D. Varies based on LDAP_refresh setting.

Answer: D

Explanation:
Reference: http://docshare02.docshare.tips/files/22651/226514302.pdf

NEW QUESTION 37
Which of the following are required when defining an index in indexes.conf? (Select all that apply.)

A. coldPath
B. homePath
C. frozenPath
D. thawedPath

Answer: D

Explanation:
Reference: https://docs.splunk.com/Documentation/Splunk/7.3.1/Admin/Indexesconf#PER_INDEX_OPTIONS

NEW QUESTION 39
What hardware attribute would you need to be changed to increase the number of simultaneous searches (ad-hoc and scheduled) on a single search head?

A. Disk
B. CPUs
C. Memory
D. Network interface cards

Answer: B

Explanation:
Reference: https://docs.splunk.com/Documentation/Splunk/7.3.1/DistSearch/SHCarchitecture

NEW QUESTION 42
With authentication methods are natively supported within Splunk Enterprise? (Select all that apply.)

A. LDAP
B. SAML
C. RADIUS
D. Duo Multifactor Authentication

Answer: AD

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

NEW QUESTION 45
.....

Thank You for Trying Our Product

We offer two products:

1st - We have Practice Tests Software with Actual Exam Questions

2nd - Questons and Answers in PDF Format

SPLK-1003 Practice Exam Features:

* SPLK-1003 Questions and Answers Updated Frequently

* SPLK-1003 Practice Questions Verified by Expert Senior Certified Staff

* SPLK-1003 Most Realistic Questions that Guarantee you a Pass on Your FirstTry

* SPLK-1003 Practice Test Questions in Multiple Choice Formats and Updatesfor 1 Year