Splunk

Exam Questions SPLK-1003

Splunk Enterprise Certified Admin

NEW QUESTION 1
Which setting in indexes.conf allows data retention to be controlled by time?

A. maxDaysToKeep
B. moveToFrozenAfter
C. maxDataRetentionTime
D. frozenTimePeriodInSecs

Answer: D

Explanation:
Reference: https://docs.splunk.com/Documentation/Splunk/7.3.1/Indexer/SmartStoredataretention

NEW 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

Answer: D

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

NEW QUESTION 3
In which Splunk configuration is the SEDCMD used?

A. props.conf
B. inputs.conf
C. indexes.conf
D. transforms.conf

Answer: A

Explanation:
Reference: https://answers.splunk.com/answers/212128/why-sedcmd-configured-in-propsconf-is-working-duri.html

NEW QUESTION 4
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 5
Which forwarder type can parse data prior to forwarding?

A. Universal forwarder
B. Heaviest forwarder
C. Hyper forwarder
D. Heavy forwarder

Answer: D

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

NEW QUESTION 6
Which Splunk component consolidates the individual results and prepares reports in a distributed environment?

A. Indexers
B. Forwarder
C. Search head
D. Search peers

Answer: A

Explanation:
Reference: https://docs.splunk.com/Documentation/Splunk/7.3.1/Indexer/Advancedindexingstrategy

NEW QUESTION 7
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 8
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 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 12
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 13
Within props.conf, which stanzas are valid for data modification? (Select all that apply.)

A. Host
B. Server
C. Source
D. Sourcetype

Answer: CD

Explanation:
Reference: https://answers.splunk.com/answers/3687/host-stanza-in-props-conf-not-being-honored-for-udp-514-data-sources.html

NEW QUESTION 14
What is the correct order of steps in Duo Multifactor Authentication?

A. * 1. Request Login* 2. Connect to SAML server* 3. Duo MFA* 4. Create User session* 5. Authentication Granted* 6. Log into Splunk
B. * 1. Request Login* 2. Duo MFA* 3. Authentication Granted* 4. Connect to SAML server* 5. Log into Splunk* 6. Create User session
C. * 1. Request Login* 2. Check authentication / group mapping* 3. Authentication Granted* 4. Duo MFA* 5. Create User session* 6. Log into Splunk
D. * 1. Request Login* 2. Duo MFA* 3. Check authentication / group mapping* 4. Create User session* 5. Authentication Granted* 6. Log into Splunk

Answer: C

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

NEW QUESTION 17
Where can scripts for scripted inputs reside on the host file system? (Select all that apply.)

A. $SPLUNK_HOME/bin/scripts
B. $SPLUNK_HOME/etc/apps/bin
C. $SPLUNK_HOME/etc/system/bin
D. $SPLUNK_HOME/etc/apps/<your_app>/bin

Answer: ACD

Explanation:
Reference: https://docs.splunk.com/Documentation/Splunk/7.3.1/Data/Getdatafromscriptedinputs#Where_to_place_the_scripts_for_scripted_inputs

NEW QUESTION 19
Which of the following are supported options when configuring optional network inputs?

A. Metadata override, sender filtering options, network input queues (quantum queues)
B. Metadata override, sender filtering options, network input queues (memory/persistent queues)
C. Filename override, sender filtering options, network output queues (memory/persistent queues)
D. Metadata override, receiver filtering options, network input queues (memory/persistent queues)

Answer: D

NEW QUESTION 20
What is the default character encoding used by Splunk during the input phase?

A. UTF-8
B. UTF-16
C. EBCDIC
D. ISO 8859

Answer: A

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

NEW QUESTION 21
How would you configure your distsearch.conf to allow you to run the search below?
sourcetype=access_combined status=200 action=purchase splunk_server_group=HOUSTON

A. [distributedSearch:NYC] default = false servers = nyc1:8089, nyc2:8089 [distributedSearch:HOUSTON] default = falseservers = houston1:8089, houston2:8089
B. [distributedSearch] servers =nyc1, nyc2, houston1, houston2 [distributedSearch:NYC] default = false servers = nyc1, nyc2 [distributedSearch:HOUSTON]default = false servers = houston1, houston2
C. [distributedSearch] servers =nyc1:8089, nyc2:8089, houston1:8089, houston2:8089[distributedSearch:NYC] default= false servers = nyc1:8089, nyc2:8089 [distributedSearch:HOUSTON]default = falseservers = houston1:8089, houston2:8089
D. [distributedSearch] servers =nyc1:8089; nyc2:8089; houston1:8089; houston2:8089[distributedSearch:NYC]default = false servers = nyc1:8089; nyc2:8089 [distributedSearch:HOUSTON] default = false servers = houston1:8089; houston2:8089

Answer: D

NEW QUESTION 24
Which Splunk component does a search head primarily communicate with?

A. Indexer
B. Forwarder
C. Cluster master
D. Deployment server

Answer: A

Explanation:
Reference: https://docs.splunk.com/Documentation/Splunk/7.3.1/InheritedDeployment/Deploymenttopology

NEW QUESTION 25
Which option accurately describes the purpose of the HTTP Event Collector (HEC)?

A. A token-based HTTP input that is secure and scalable and that requires the use of forwarders.
B. A token-based HTTP input that is secure and scalable and that does not require the use of forwarders.
C. An agent-based HTTP input that is secure and scalable and that does not require the use of forwarders.
D. A token-based HTTP input that is insecure and non-scalable and that does not require the use of forwarders.

Answer: B

Explanation:
Reference: http://dev.splunk.com/view/event-collector/SP-CAAAE6M

NEW QUESTION 29
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 31
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 33
In which scenario would a Splunk Administrator want to enable data integrity check when creating an index?

A. To ensure that hot buckets are still open for writers and have not been forced to roll to a cold state.
B. To ensure that configuration files have not been tampered with for auditing and/or legal purposes.
C. To ensure that user passwords have not been tampered with for auditing and/or legal purposes.
D. To ensure that data has not been tampered with for auditing and/or legal purposes.

Answer: D

Explanation:
Reference: https://www.splunk.com/blog/2015/10/28/data-integrity-is-back-baby.html

NEW QUESTION 37
Which Splunk component performs indexing and responds to search requests from the search head?

A. Forwarder
B. Search peer
C. License master
D. Search head cluster

Answer: B

Explanation:
Reference: https://www.edureka.co/blog/splunk-architecture/

NEW QUESTION 42
Which of the following apply to how distributed search works? (Select all that apply.)

A. The search head dispatches searches to the peers.
B. The search peers pull the data from the forwarders.
C. Peers run searches in parallel and return their portion of results.
D. The search head consolidates the individual results and prepares reports.

Answer: A

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

NEW QUESTION 45
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 50
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 55
.....

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