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
In case of a conflict between a whitelist and a blacklist input setting, which one is used?

A. Blacklist
B. Whitelist
C. They cancel each other out.
D. Whichever is entered into the configuration first.

Answer: A

Explanation:
Reference: https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=8&ved=2ahUKEwj0r6Lso6bkAhUqxYUKHbWlDz4QFjAHegQIAxAC&url=http%3A%2F%2Fsplunk.training%2Fshowpdf.asp%3Fdata%3D789BB6B10C1B4376B548D711B4377F3F4B511B437805A8EC11B437742EA8F11B43779B6FA211B4376EA657C11B4376FC19B311B4377E2407E11B43730AF97411B4377F3F4B511B437742EA8F11B43779B6FA211B43771F822111B437731365811B43730AF97411B437789BB6B11B4376B548D711B4377F3F4B511B437805A8EC11B437742EA8F11B43779B6FA211B4376EA657C11B4376FC19B311B4377E2407E11B43732E61E211B4377F3F4B511B437742EA8F11B43779B6FA211B43771F822111B437731365811B43746D0DC011B4377549EC611B4377BED81011B437789BB6B11B4376D8B14511B437731365811B4376B548D711B4377F3F4B511B4376FC19B311B43732E61E211B4376D8B14511B4377AD23D911B437789BB6B11B43730AF97411B4373989B2C11B437386E6F511B437386E6F511B4373DF6C0811B43737532BE11B4373BC039A11B437351CA5011B43737532BE11B43730AF97411B4375BD6DD511B43730AF97411B437564E8C211B43730AF97411B437%257C2318D1%257C11649A&usg=AOvVaw2e9s-JweivuCkqTb4-Y9uW

NEW QUESTION 3
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 4
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 5
In which phase of the index time process does the license metering occur?

A. Input phase
B. Parsing phase
C. Indexing phase
D. Licensing phase

Answer: C

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

NEW QUESTION 6
The priority of layered Splunk configuration files depends on the file's:

A. Owner
B. Weight
C. Context
D. Creation time

Answer: C

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

NEW QUESTION 7
What is required when adding a native user to Splunk? (Select all that apply.)

A. Password
B. Username
C. Full Name
D. Default app

Answer: CD

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

NEW QUESTION 8
Which Splunk forwarder type allows parsing of data before forwarding to an indexer?

A. Universal forwarder
B. Parsing forwarder
C. Heavy forwarder
D. Advanced forwarder

Answer: C

Explanation:
Reference: https://docs.splunk.com/Documentation/SplunkCloud/7.2.6/Forwarding/Typesofforwarders

NEW QUESTION 9
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 10
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 10
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 14
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 17
Which of the following is a valid distributed search group?

A. [distributedSearch:Paris] default = false servers = server1, server2
B. [searchGroup:Paris] default = false servers = server1:8089, server2:8089
C. [searchGroup:Paris] default = false servers = server1:9997, server2:9997
D. [distributedSearch:Paris] default = false servers = server1:8089; server2:8089

Answer: D

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

NEW QUESTION 20
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 of the following are methods for adding inputs in Splunk? (Select all that apply.)

A. CLI
B. Splunk Web
C. Editing inpits.conf
D. Editing monitor.conf

Answer: AB

Explanation:
Reference: http://dev.splunk.com/view/dev -guide/SP-CAAAE3A

NEW QUESTION 28
Which valid bucket types are searchable? (Select all that apply.)

A. Hot buckets
B. Cold buckets
C. Warm buckets
D. Frozen buckets

Answer: ABC

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

NEW QUESTION 31
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 34
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 35
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 40
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 44
.....

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