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%3D789BB6B10C1B4376B548D711B4377F3F4B511B437805A8EC11B437742EA8F11B43779B6FA211B4376
EA657C11B4376FC19B311B4377E2407E11B43730AF97411B4377F3F4B511B437742EA8F11B43779B6FA211B43771F822111B437731365811B43730AF9741
1B437789BB6B11B4376B548D711B4377F3F4B511B437805A8EC11B437742EA8F11B43779B6FA211B4376EA657C11B4376FC19B311B4377E2407E11B437
32E61E211B4377F3F4B511B437742EA8F11B43779B6FA211B43771F822111B437731365811B43746D0DC011B4377549EC611B4377BED81011B437789BB6
B11B4376D8B14511B437731365811B4376B548D711B4377F3F4B511B4376FC19B311B43732E61E211B4376D8B14511B4377AD23D911B437789BB6B11B43
730AF97411B4373989B2C11B437386E6F511B437386E6F511B4373DF6C0811B43737532BE11B4373BC039A11B437351CA5011B43737532BE11B43730AF9
7411B4375BD6DD511B43730AF97411B437564E8C211B43730AF97411B437%257C2318D1%257C11649A&usg=AOvVaw2e9s-JweivuCkqTb4-Y9uW

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 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 5
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 6
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 7
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 8
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 9
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 10
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 10
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 12
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 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 20
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 22
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 24
For single line event sourcetypes, it is most efficient to set SHOULD_LINEMERGE
to what value?

A. True
B. False
C. <regex string>
D. Newline Character

Answer: B

Explanation:
Reference: https://answers.splunk.com/answers/704533/what-are-the-best-practices-for-defining-source-ty.html

NEW QUESTION 29
Which of the following authentication types requires scripting in Splunk?

A. ADFS
B. LDAP
C. SAML
D. RADIUS

Answer: D

Explanation:
Reference: https://answers.splunk.com/answers/131127/scripted-authentication.html

NEW QUESTION 34
What are the required stanza attributes when configuring the transforms.conf to manipulate or remove events?

A. REGEX, DEST, FORMAT
B. REGEX, SRC_KEY, FORMAT
C. REGEX, DEST_KEY, FORMAT
D. REGEX, DEST_KEY, FORMATTING

Answer: C

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

NEW QUESTION 38
Which of the following indexes come pre-configured with Splunk Enterprise? (Select all that apply.)

A. _licence
B. _internal
C. _external
D. _thefishbucket

Answer: B

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

NEW QUESTION 42
Where are license files stored?

A. $SPLUNK_HOME/etc/secure
B. $SPLUNK_HOME/etc/system
C. $SPLUNK_HOME/etc/licenses
D. $SPLUNK_HOME/etc/apps/licenses

Answer: C

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

NEW QUESTION 46
When deploying apps, which attribute in the forwarder management interface determines the apps that clients install?

A. App Class
B. Client Class
C. Server Class
D. Forwarder Class

Answer: C

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

NEW QUESTION 49
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 53
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 55

......

About Exambible

Your Partner of IT Exam

Found in 1998

Exambible is a company specialized on providing high quality IT exam practice study materials, especially Cisco CCNA, CCDA, CCNP, CCIE, Checkpoint CCSE, CompTIA A+, Network+ certification practice exams and so on. We guarantee that the candidates will not only pass any IT exam at the first attempt but also get profound understanding about the certificates they have got. There are so many alike companies in this industry, however, Exambible has its unique advantages that other companies could not achieve.

Our Advances

* 99.9% Uptime

    All examinations will be up to date.

* 24/7 Quality Support

    We will provide service round the clock.

* 100% Pass Rate

    Our guarantee that you will pass the exam.

* Unique Gurantee

    If you do not pass the exam at the first time, we will not only arrange FULL REFUND for you, but also provide you another exam of your claim, ABSOLUTELY FREE!

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%3D789BB6B10C1B4376B548D711B4377F3F4B511B437805A8EC11B437742EA8F11B43779B6FA211B4376
EA657C11B4376FC19B311B4377E2407E11B43730AF97411B4377F3F4B511B437742EA8F11B43779B6FA211B43771F822111B437731365811B43730AF9741
1B437789BB6B11B4376B548D711B4377F3F4B511B437805A8EC11B437742EA8F11B43779B6FA211B4376EA657C11B4376FC19B311B4377E2407E11B437
32E61E211B4377F3F4B511B437742EA8F11B43779B6FA211B43771F822111B437731365811B43746D0DC011B4377549EC611B4377BED81011B437789BB6
B11B4376D8B14511B437731365811B4376B548D711B4377F3F4B511B4376FC19B311B43732E61E211B4376D8B14511B4377AD23D911B437789BB6B11B43
730AF97411B4373989B2C11B437386E6F511B437386E6F511B4373DF6C0811B43737532BE11B4373BC039A11B437351CA5011B43737532BE11B43730AF9
7411B4375BD6DD511B43730AF97411B437564E8C211B43730AF97411B437%257C2318D1%257C11649A&usg=AOvVaw2e9s-JweivuCkqTb4-Y9uW

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 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 5
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 6
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 7
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 8
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 9
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 10
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 10
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 12
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 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 20
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 22
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 24
For single line event sourcetypes, it is most efficient to set SHOULD_LINEMERGE
to what value?

A. True
B. False
C. <regex string>
D. Newline Character

Answer: B

Explanation:
Reference: https://answers.splunk.com/answers/704533/what-are-the-best-practices-for-defining-source-ty.html

NEW QUESTION 29
Which of the following authentication types requires scripting in Splunk?

A. ADFS
B. LDAP
C. SAML
D. RADIUS

Answer: D

Explanation:
Reference: https://answers.splunk.com/answers/131127/scripted-authentication.html

NEW QUESTION 34
What are the required stanza attributes when configuring the transforms.conf to manipulate or remove events?

A. REGEX, DEST, FORMAT
B. REGEX, SRC_KEY, FORMAT
C. REGEX, DEST_KEY, FORMAT
D. REGEX, DEST_KEY, FORMATTING

Answer: C

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

NEW QUESTION 38
Which of the following indexes come pre-configured with Splunk Enterprise? (Select all that apply.)

A. _licence
B. _internal
C. _external
D. _thefishbucket

Answer: B

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

NEW QUESTION 42
Where are license files stored?

A. $SPLUNK_HOME/etc/secure
B. $SPLUNK_HOME/etc/system
C. $SPLUNK_HOME/etc/licenses
D. $SPLUNK_HOME/etc/apps/licenses

Answer: C

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

NEW QUESTION 46
When deploying apps, which attribute in the forwarder management interface determines the apps that clients install?

A. App Class
B. Client Class
C. Server Class
D. Forwarder Class

Answer: C

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

NEW QUESTION 49
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 53
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 55

......

Relate Links

100% Pass Your SPLK-1003 Exam with Exambible Prep Materials

https://www.exambible.com/SPLK-1003-exam/

Contact us

We are proud of our high-quality customer service, which serves you around the clock 24/7.

Viste - https://www.exambible.com/