Vendor: Splunk

Exam Code: SPLK-3003

Exam Name: Splunk Core Certified Consultant

Version: DEMO

QUESTION 1
What is the primary driver behind implementing indexer clustering in a customer's environment?

A. To improve resiliency as the search load increases.
B. To reduce indexing latency.
C. To scale out a Splunk environment to offer higher performance capability.
D. To provide higher availability for buckets of data.

Answer: D
Explanation:
https://docs.splunk.com/Documentation/Splunk/8.1.0/Indexer/Howclusteredsearchworks

QUESTION 2
In a single indexer cluster, where should the Monitoring Console (MC) be installed?

A. Deployer sharing with master cluster.
B. License master that has 50 clients or more.
C. Cluster master node
D. Production Search Head

Answer: C
Explanation:
https://docs.splunk.com/Documentation/Splunk/8.1.0/DMC/WheretohostDMC
The master node, if the load on the master node is below the limits specified in Additional roles for the master node in the Managing Indexers and Clusters of Indexers manual. Otherwise, run the monitoring console on a search head node that is dedicated to running monitoring console searches. If you are using SmartStore you must host the monitoring console on a dedicated search head.

QUESTION 3
A customer has downloaded the Splunk App for AWS from Splunkbase and installed it in a search head cluster following the instructions using the deployer. A power user modifies a dashboard in the app on one of the search head cluster members. The app containing an updated dashboard is upgraded to the latest version by following the instructions via the deployer. What happens?

A. The updated dashboard will not be deployed globally to all users, due to the conflict with the power user's modified version of the dashboard.
B. Applying the search head cluster bundle will fail due to the conflict.
C. The updated dashboard will be available to the power user.
D. The updated dashboard will not be available to the power user; they will see their modified version.

Answer: D
Explanation:
When a user have a role that can modify a dashboard, if he do it, the original xml file is untouched and stay in "default" folder but the new one is in "local" folder and take precedence over the one in "default".
When the app is updated, the original file is updated BUT the file in local is untouched and still have precedence (tested right now on a dev platform).

QUESTION 4
A customer's deployment server is overwhelmed with forwarder connections after adding an additional 1000 clients. The default phone home interval is set to 60 seconds. To reduce the number of connection failures to the DS what is recommended?

A. Create a tiered deployment server topology.
B. Reduce the phone home interval to 6 seconds.
C. Leave the phone home interval at 60 seconds.
D. Increase the phone home interval to 600 seconds.

Answer: D
Explanation:
IE slowing down the phone home time to 10 minutes would slow down the connection collisions. Third option not here would be to use DNS name for the DS then utilize Round Robin or some other type of Load Balancing to handle connection requests.

QUESTION 5
Which of the following server.conf stanzas indicates the Indexer Discovery feature has not been fully configured (restart pending) on the Master Node?

A.
```
[indexer_discovery]
pass4SymmKey = $7$XcXl1lu3820Jbui14oVe324+mvx6gCKKv6kf2zEaVB6Ie4DcZ647CnLVlfW
```

B.
```
[clustering]
mode = master
pass4SymmKey = $7$tYTXzke+1r+3DULTHHDUTmYOXdtZJPxm21XwMARrJE20jsmicp9C3ni0
```

C.
```
[indexer_discovery]
pass4SymmKey = idxdiscovery
```

D.
```
[clustering]
mode = forwarder
pass4SymmKey = $7$PU9SBXww63Vz3UJdDYGIN0UrdscRh83ssC2pEpwE6P3gn50iNF094g==
```

Answer: C
Explanation:
https://docs.splunk.com/Documentation/Splunk/8.1.0/Indexer/indexerdiscovery

QUESTION 6
What is the Splunk PS recommendation when using the deployment server and building deployment apps?

A. Carefully design smaller apps with specific configuration that can be reused.
B. Only deploy Splunk PS base configurations via the deployment server.
C. Use $SPLUNK_HOME/etc/system/local configurations on forwarders and only deploy TAs via the deployment server.
D. Carefully design bigger apps containing multiple configs.

Answer: A

QUESTION 7

Which of the following processor occur in the indexing pipeline?

A. tcp out, syslog out
B. Regex replacement, annotator
C. Aggregator
D. UTF-8, linebreaker, header

Answer: A
Explanation:
IndexPipe: Tcpout to another Splunk, syslog output, and indexing are done here.
In addition, this pipeline is responsible for bytequota, block signing, and indexing metrics such as thruput etc.
https://wiki.splunk.com/Community:HowIndexingWorks

QUESTION 8
Which configuration item should be set to false to significantly improve data ingestion performance?

A. AUTO_KV_JSON
B. BREAK_ONLY_BEFORE_DATE
C. SHOULD_LINEMERGE
D. ANNOTATE_PUNCT

Answer: C
Explanation:
https://docs.splunk.com/Documentation/Splunk/8.0.6/Data/Configureeventlinebreaking

QUESTION 9
A customer has a new set of hardware to replace their aging indexers. What method would reduce the amount of bucket replication operations during the migration process?

A. Disable the indexing ports on the old indexers.
B. Disable replication ports on the old indexers.
C. Put the old indexers into manual detention.
D. Put the old indexers into automatic detention.

Answer: C
Explanation:
https://docs.splunk.com/Documentation/Splunk/latest/Indexer/Peerdetention?#Manual_detention

QUESTION 10
When a bucket rolls from cold to frozen on a clustered indexer, which of the following scenarios occurs?

A. All replicated copies will be rolled to frozen; original copies will remain.
B. Replicated copies of the bucket will remain on all other indexers and the Cluster Master (CM) assigns a new primary bucket.
C. The bucket rolls to frozen on all clustered indexers simultaneously.
D. Nothing. Replicated copies of the bucket will remain on all other indexers until a local retention rule causes it to roll.3

Answer: B
Explanation:
https://docs.splunk.com/Documentation/Splunk/8.1.0/Indexer/Bucketsandclusters

QUESTION 11
A site from a multi-site indexer cluster needs to be decommissioned. Which of the following actions must be taken?

A. Nothing. Decommissioning a site is not possible.
B. Create an alias for where the new data should be sent.
C. Remove the site from the list of available sites.
D. Remove the site from the list of available sites and create an alias for where the new data should be sent.

Answer: D
Explanation:
https://docs.splunk.com/Documentation/Splunk/8.1.1/Indexer/Decommissionasite

QUESTION 12
A customer wants to implement LDAP because managing local Splunk users is becoming too much of an overhead. What configuration details are needed from the customer to implement LDAP authentication?

A. API: Python script with PAM/RADIUS details.
B. LDAP server: port, bind user credentials, path/to/groups, path/to/user.
C. LDAP server: port, bind user credentials, base DN for groups, base DN for users.
D. LDAP REST details, base DN for groups, base DN for users.

Answer: C
Explanation:
https://docs.splunk.com/Documentation/Splunk/8.1.1/Security/ConfigureLDAPwithSplunkWeb

QUESTION 13
A customer has a search cluster (SHC) of six members split evenly between two data centers (DC). The customer is concerned with network connectivity between the two DCs due to frequent outages. Which of the following is true as it relates to SHC resiliency when a network outage occurs between the two DCs?

A. The SHC will function as expected as the SHC deployer will become the new captain until the network communication is restored.
B. The SHC will stop all scheduled search activity within the SHC.
C. The SHC will function as expected as the minimum required number of nodes for a SHC is 3.
D. The SHC will function as expected as the SHC captain will fall back to previous active captain in the remaining site.

Answer: B
Explanation:
https://docs.splunk.com/Documentation/Splunk/8.2.1/DistSearch/DeploymultisiteSHC

Thank You for Trying Our Product

Lead2pass Certification Exam Features:

★ More than **99,900** Satisfied Customers Worldwide.

★ Average **99.9%** Success Rate.

★ **Free Update** to match latest and real exam scenarios.

★ **Instant Download** Access! No Setup required.

★ Questions & Answers are downloadable in **PDF** format and **VCE** test engine format.

★ Multi-Platform capabilities - **Windows, Laptop, Mac, Android, iPhone, iPod, iPad**.

★ **100%** Guaranteed Success or **100%** Money Back Guarantee.

★ **Fast**, helpful support **24x7**.

View list of all certification exams: http://www.lead2pass.com/all-products.html

10% Discount Coupon Code: **ASTR14**