Vendor: Splunk

Exam Code: SPLK-1003

Exam Name: Splunk Enterprise Certified Admin

Version: DEMO

QUESTION 1
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: C
Explanation:
https://docs.splunk.com/Documentation/Splunk/8.0.5/Updating/Updateconfigurations
The deployment server distributes deployment apps to clients.

QUESTION 2
Where should apps be located on the deployment server that the clients pull from?

A. $SFLUNK_KOME/etc/apps
B. $SPLUNK_HCME/etc/sear:ch
C. $SPLUNK_HCME/etc/master-apps
D. $SPLUNK HCME/etc/deployment-apps

Answer: D
Explanation:
After an app is downloaded, it resides under $SPLUNK_HOME/etc/apps on the deployment clients. But it resided in the $SPLUNK_HOME/etc/deployment-apps location in the deployment server.

QUESTION 3
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: B

QUESTION 4
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:
"When ingesting event data, the measured data volume is based on the new raw data that is placed into the indexing pipeline. Because the data is measured at the indexing pipeline, data that is filetered and dropped prior to indexing does not count against the license volume qota."
https://docs.splunk.com/Documentation/Splunk/8.0.6/Admin/HowSplunklicensingworks

QUESTION 5
You update a props. conf file while Splunk is running. You do not restart Splunk and you run this command: splunk btoo1 props list --debug. What will the output be?

A. list of all the configurations on-disk that Splunk contains.
B. A verbose list of all configurations as they were when splunkd started.
C. A list of props. conf configurations as they are on-disk along with a file path from which the configuration is located
D. A list of the current running props, conf configurations along with a file path from which the configuration was made

Answer: C
Explanation:
https://docs.splunk.com/Documentation/Splunk/8.0.1/Troubleshooting/Usebtooltotroubleshootconfigurations
"The btool command simulates the merging process using the on-disk conf files and creates a report showing the merged settings."
"The report does not necessarily represent what's loaded in memory. If a conf file change is made that requires a service restart, the btool report shows the change even though that change isn't active."

QUESTION 6
When running the command shown below, what is the default path in which deployment server. conf is created?
splunk set deploy-poll deployServer:port

A. SFLUNK_HOME/etc/deployment
B. SPLUNK_HOME/etc/system/local

C. SPLUNK_HOME/etc/system/default
D. SPLUNK_KOME/etc/apps/deployment

Answer: C
Explanation:
https://docs.splunk.com/Documentation/Splunk/8.1.1/Updating/Definedeploymentclasses#Ways_to_define_server_classes
"When you use forwarder management to create a new server class, it saves the server class definition in a copy of serverclass.conf under $SPLUNK_HOME/etc/system/local. If, instead of using forwarder management, you decide to directly edit serverclass.conf, it is recommended that you create the serverclass.conf file in that same directory, $SPLUNK_HOME/etc/system/local."

QUESTION 7
The priority of layered Splunk configuration files depends on the file's:

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

Answer: C
Explanation:
https://docs.splunk.com/Documentation/Splunk/7.3.0/Admin/Wheretofindtheconfigurationfiles
To determine the order of directories for evaluating configuration file precendence, Splunk software considers each file's context. Configuration files operate in either a global context or in the context of the current app and user.

QUESTION 8
When configuring monitor inputs with whitelists or blacklists, what is the supported method of filtering the lists?

A. Slash notation
B. Regular expression
C. Irregular expression
D. Wildcard-only expression

Answer: B

QUESTION 9
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: AB
Explanation:
According to the Splunk system admin course PDF, When adding native users, Username and Password ARE REQUIRED

QUESTION 10
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:
https://docs.splunk.com/Documentation/Splunk/8.0.5/Admin/Inputsconf

QUESTION 11
Which Splunk component requires a Forwarder license?

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

Answer: B

QUESTION 12
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:
https://docs.splunk.com/Documentation/Splunk/7.0.3/Forwarding/Routeandfilterdatad#Perform_selective_indexing_and_forwarding
Specifies a comma-separated list of tcpout group names. Use this setting to selectively forward your data to specific indexers by specifying the tcpout groups that the forwarder should use when forwarding the data. Define the tcpout group names in the outputs.conf file in [tcpout:<tcpout_group_name>] stanzas. The groups present in defaultGroup in [tcpout] stanza in the outputs.conf file.

QUESTION 13
To set up a Network input in Splunk, what needs to be specified'?

A. File path.
B. Username and password
C. Network protocol and port number.
D. Network protocol and MAC address.

Answer: C
Explanation:
https://docs.splunk.com/Documentation/Splunk/8.0.3/Data/Monitornetworkports

QUESTION 14
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

QUESTION 15
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: AB
Explanation:
https://docs.splunk.com/Documentation/Splunk/8.2.2/Admin/Distdeploylicenses#:~:text=License%2 0requirements,do%20not%20index%20external%20data.
"All Splunk Enterprise instances functioning as management components needs access to an Enterprise license. Management components include the deployment server, the indexer cluster manager node, the search head cluster deployer, and the monitoring console."
https://docs.splunk.com/Documentation/Splunk/8.2.2/Updating/Aboutdeploymentserver
"The deployment server is the tool for distributing configurations, apps, and content updates to groups of Splunk Enterprise instances."

QUESTION 16
During search time, which directory of configuration files has the highest precedence?

A. $SFLUNK_KOME/etc/system/local
B. $SPLUNK_KCME/etc/system/default
C. $SPLUNK_HCME/etc/apps/app1/local
D. $SPLUNK HCME/etc/users/admin/local

Answer: D
Explanation:
"To keep configuration settings consistent across peer nodes, configuration files are managed from the cluster master, which pushes the files to the slave-app directories on the peer nodes. Files in the slave-app directories have the highest precedence in a cluster peer's configuration. Here is the expanded precedence order for cluster peers:
1.Slave-app local directories --highest priority
2. System local directory
3. App local directories
4. Slave-app default directories

5. App default directories
6. System default directory --lowest priority

QUESTION 17
Within props. conf, which stanzas are valid for data modification? (select all that apply)

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

Answer: ACD
Explanation:
Reuse of the same field-extracting regular expression across multiple sources, source types, or hosts.
https://docs.splunk.com/Documentation/Splunk/8.0.4/Admin/Propsconf#props.conf.spec

QUESTION 18
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:
Scroll down to the Network Diagram section and note the following 6 similar steps
1 -SPlunk connection initiated
2 -Primary authentication
3 -Splunk connection established to Duo Security over TCP port 443
4 -Secondary authentication via Duo Security's service
5 -Splunk receives authentication response
6 -Splunk session logged in.

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**