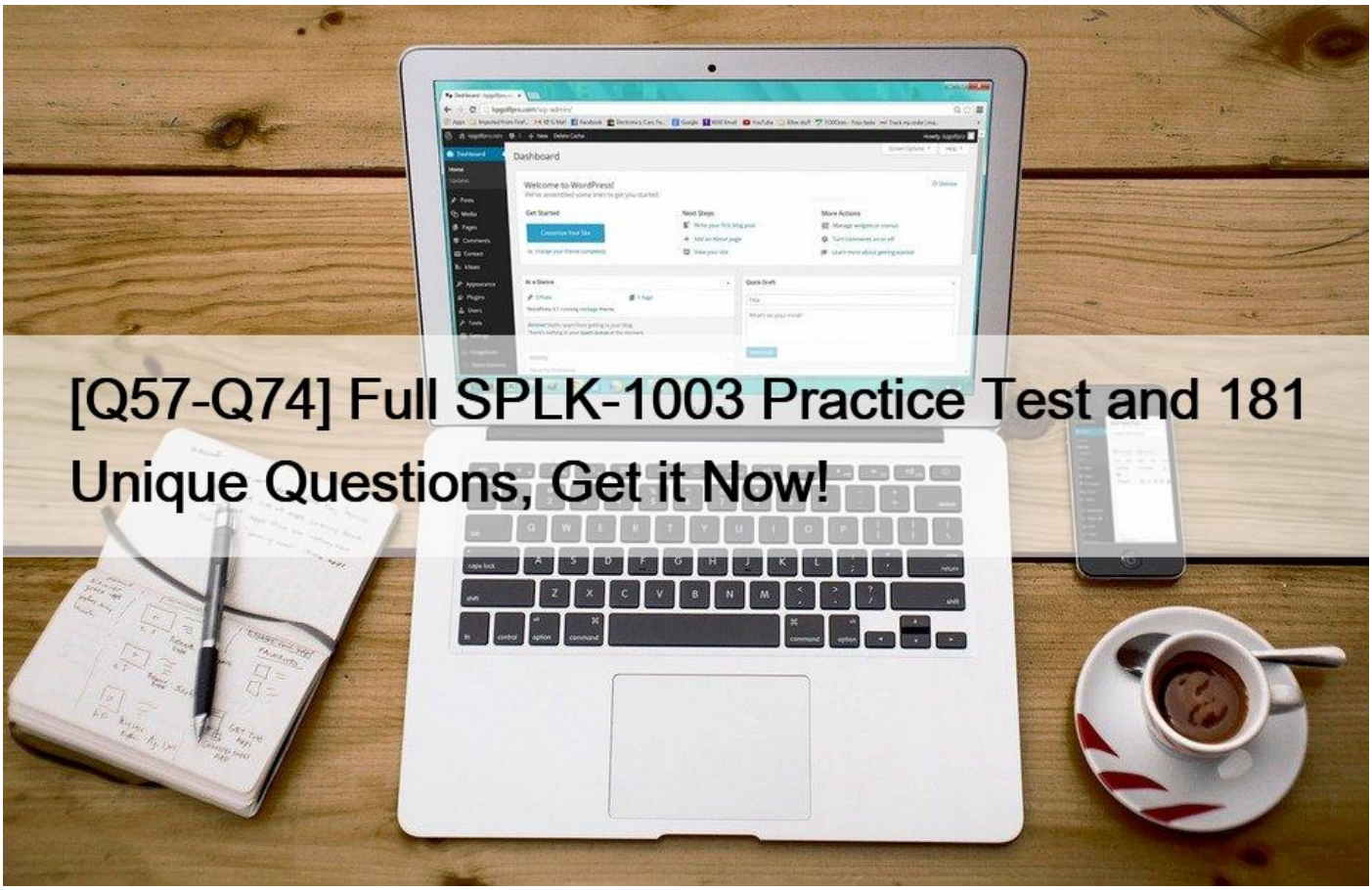
[Q57-Q74 Full SPLK-1003 Practice Test and 181 Unique Questions, Get it Now!



Full SPLK-1003 Practice Test and 181 Unique Questions, Get it Now!
The Best SPLK-1003 Exam Study Material Premium Files and Preparation Tool

Splunk SPLK-1003 (Splunk Enterprise Certified Admin) certification exam is designed for IT professionals who want to validate their skills and knowledge on deploying, managing, and troubleshooting Splunk Enterprise. Splunk Enterprise Certified Admin certification is recognized globally and is ideal for individuals who are responsible for the day-to-day administration of Splunk, including creating and managing data inputs, configuring users and roles, and troubleshooting common issues.

NEW QUESTION 57

A new forwarder has been installed with a manually created deploymentclient.conf.

What is the next step to enable the communication between the forwarder and the deployment server?
* Restart Splunk on the deployment server.
* Enable the deployment client in Splunk Web under Forwarder Management.
* Restart Splunk on the deployment client.
* Wait for up to the time set in the phoneHomeIntervalInSecs setting.

The next step to enable the communication between the forwarder and the deployment server after installing a new forwarder with a manually created deploymentclient.conf is to restart Splunk on the deployment client. The deploymentclient.conf file contains the settings for the deployment client, which is a Splunk instance that receives updates from the deployment server. The file must include the targetUri attribute, which specifies the hostname and management port of the deployment server. To apply the changes in the deploymentclient.conf file, Splunk must be restarted on the deployment client. Therefore, option C is the correct answer. Reference: Splunk Enterprise Certified Admin | Splunk, [Configure deployment clients – Splunk Documentation]

NEW QUESTION 58

The universal forwarder has which capabilities when sending data? (select all that apply)
* Sending alerts
* Compressing data
* Obfuscating/hiding data
* Indexer acknowledgement

https://docs.splunk.com/Documentation/Splunk/8.0.1/Forwarding/Aboutforwardingandreceivingdata

https://docs.splunk.com/Documentation/Forwarder/8.1.1/Forwarder/Configureforwardingwithoutputs.conf#:~:text=compressed%3Dtrue%20This%20tells%20the,the%20forwarder%20sends%20raw%20data.

NEW QUESTION 59

Which of the following are required when defining an index in indexes. conf? (select all that apply)
* coldPath
* homePath
* frozenPath
* thawedPath

NEW QUESTION 60

Which of the following is a valid distributed search group?
* [distributedSearch:Paris] default = false servers = server1, server2
* [searchGroup:Paris] default = false servers = server1:8089, server2:8089
* [searchGroup:Paris] default = false servers = server1:9997, server2:9997
* [distributedSearch:Paris] default = false servers = server1:8089; server2:8089

https://docs.splunk.com/Documentation/Splunk/9.0.0/DistSearch/Distributedsearchgroups

NEW QUESTION 61

When indexing a data source, which fields are considered metadata?
* source, host, time
* time, sourcetype, source
* host, raw, sourcetype
* sourcetype, source, host

NEW QUESTION 62

Which of the following must be done to define user permissions when integrating Splunk with LDAP?
* Map Users
* Map Groups
* Map LDAP Inheritance

* Map LDAP to Active Directory
https://docs.splunk.com/Documentation/Splunk/8.1.3/Security/ConfigureLDAPwithSplunkWeb

“You can map either users or groups, but not both. If you are using groups, all users must be members of an appropriate group. Groups inherit capabilities form the highest level role they’re a member of.” “If your LDAP environment does not have group entries, you can treat each user as its own group.”

NEW QUESTION 63

What is the correct curl to send multiple events through HTTP Event Collector?

```
curl "https://mysplunkserver.example.com:8088/services/collector" \
-H "Authorization: Splunk DF457ZE4-3G51-85F5-H777-0284GG91PF67" \
-d "event": "Hello World", "Hola Mundo", "Hallo Welt"
```

```
curl "https://mysplunkserver.example.com:8088/services/collector" \
-H "Authorization: Splunk DF457ZE4-3G51-85F5-H777-0284GG91PF67" \
-d "event": "Hello World", "event": "Hola Mundo", "event": "Hallo Welt"
```

```
curl "https://mysplunkserver.example.com:8088/services/collector" \
-H "Authorization: Splunk DF457ZE4-3G51-85F5-H777-0284GG91PF67" \
-d '{"event": "Hello World"}{"event": "Hola Mundo"}{"event": "Hallo Welt", "nested":
```

```
curl "https://mysplunkserver.example.com:8088/services/collector" \
-H "Authorization: Splunk DF457ZE4-3G51-85F5-H777-0284GG91PF67" \
-d '{"event": "Hello World", "Hola Mundo", "Hallo Welt", "nested": {"key1": "value1"
```


* Option A
* Option B
* Option C
* Option D
Explanation

curl “https://mysplunkserver.example.com:8088/services/collector” -H “Authorization: Splunk DF4S7ZE4-3GS1-8SFS-E777-0284GG91PF67” -d ‘{“event”: “Hello World”}, {“event”: “Hola Mundo”},

{“event”: “Hallo Welt”}’. This is the correct curl command to send multiple events through HTTP Event Collector (HEC), which is a token-based API that allows you to send data to Splunk Enterprise from any application that can make an HTTP request. The command has the following components:

* The URL of the HEC endpoint, which consists of the protocol (https), the hostname or IP address of the Splunk server (mysplunkserver.example.com), the port number (8088), and the service name (services/collector).

* The header that contains the authorization token, which is a unique identifier that grants access to the HEC endpoint. The token is prefixed with Splunk and enclosed in quotation marks. The token value (DF4S7ZE4-3GS1-8SFS-E777-0284GG91PF67) is an

example and should be replaced with your own token value.

* The data payload that contains the events to be sent, which are JSON objects enclosed in curly braces and separated by commas. Each event object has a mandatory field called event, which contains the raw data to be indexed. The event value can be a string, a number, a boolean, an array, or another JSON object. In this case, the event values are strings that say hello in different languages.

NEW QUESTION 64

What are the minimum required settings when creating a network input in Splunk?
* Protocol, port number
* Protocol, port, location
* Protocol, username, port
* Protocol, IP. port number
https://docs.splunk.com/Documentation/Splunk/8.0.5/Admin/Inputsconf

[tcp://<remote server>:<port>]

*Configures the input to listen on a specific TCP network port.

*If a <remote server> makes a connection to this instance, the input uses this stanza to configure itself.

*If you do not specify <remote server>, this stanza matches all connections on the specified port.

*Generates events with source set to “tcp:<port>”, for example: tcp:514

*If you do not specify a sourcetype, generates events with sourcetype set to “tcp-raw”

NEW QUESTION 65

A non-clustered Splunk environment has three indexers (A,B,C) and two search heads (X, Y). During a search executed on search head X, indexer A crashes. What is Splunk’s response?
* Update the user in Splunk web informing them that the results of their search may be incomplete.
* Repeat the search request on indexer B without informing the user.
* Update the user in Splunk web that their results may be incomple and that Splunk will try to re-execute the search.
* Inform the user in Splunk web that their results may be incomplete and have them attempt the search from search head Y.
Explanation

This is explained in the Splunk documentation1, which states:

If an indexer goes down during a search, the search head notifies you that the results might be incomplete.

The search head does not attempt to re-run the search on another indexer.

NEW QUESTION 66

In addition to single, non-clustered Splunk instances, what else can the deployment server push apps to?
* Universal forwarders
* Splunk Cloud
* Linux package managers
* Windows using WMI

Reference:

The deployment server is a Splunk component that distributes apps and other configurations to deployment clients, which are Splunk instances that receive updates from the deployment server. The deployment server can push apps to single, non-clustered Splunk instances, as well as universal forwarders, which are lightweight Splunk agents that forward data to indexers. Therefore, option A is the correct answer. Reference: Splunk Enterprise Certified Admin | Splunk, [About deployment server and forwarder management – Splunk Documentation]

NEW QUESTION 67

The universal forwarder has which capabilities when sending data? (select all that apply)
* Sending alerts
* Compressing data
* Obfuscating/hiding data
* Indexer acknowledgement

Explanation

https://docs.splunk.com/Documentation/Splunk/8.0.1/Forwarding/Aboutforwardingandreceivingdata

https://docs.splunk.com/Documentation/Forwarder/8.1.1/Forwarder/Configureforwardingwithoutputs.conf#:~:tex

NEW QUESTION 68

Which of the following statements describe deployment management? (Choose all that apply.)
* Requires an Enterprise license.
* Is responsible for sending apps to forwarders.
* Once used, is the only way to manage forwarders.
* Can automatically restart the host OS running the forwarder.

NEW QUESTION 69

An add-on has configured field aliases for source IP address and destination IP address fields. A specific user prefers not to have those fields present in their user context. Based on the default props.conf below, which SPLUNK_HOME/etc/users/buttercup/myTA/local/props.conf stanza can be added to the user’s local context to disable the field aliases?

```
SPLUNK_HOME/etc/apps/myTA/default/props.conf
[mySourcetype]
FIELDALIAS-cim-src_ip = sourceIPAddress as src_ip
FIELDALIAS-cim-dest-ip = destinationIPaddress as dest_ip
```

A.
```
[mySourcetype]
disable FIELDALIAS-cim-src_ip
disable FIELDALIAS-cim-dest-ip
```

B.
```
[mySourcetype]
FIELDALIAS-cim-src_ip =
FIELDALIAS-cim-dest-ip
```

C.
```
[mySourcetype]
unset FIELDALIAS-cim-src_ip
unset FIELDALIAS-cim-dest-ip
```

D.
```
[mySourcetype]
#FIELDALIAS-cim-src_ip = sourceIPAddress as src_ip
#FIELDALIAS-cim-dest-ip = destinationIPaddress as dest_ip
```


* Option A
* Option B
* Option C
* Option D

https://docs.splunk.com/Documentation/Splunk/latest/Admin/Howtoeditaconfigurationfile#Clear%20a%20setting

NEW QUESTION 70

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?

* /var/log/messages
* /var/log/maillog
* /var/log/maillog and /var/log/messages
* none of the above

NEW QUESTION 71

Which forwarder is recommended by Splunk to use in a production environment?
* Heavy forwarder
* SSL forwarder
* Lightweight forwarder
* Universal forwarder

Reference:

The forwarder that is recommended by Splunk to use in a production environment is the universal forwarder. The universal forwarder is a lightweight Splunk agent that forwards data to indexers or other forwarders. The universal forwarder has a small footprint and consumes minimal system resources. It also supports secure and reliable data forwarding with encryption and acknowledgement features. Therefore, option D is the correct answer. Reference: Splunk Enterprise Certified Admin | Splunk, [About forwarding and receiving data – Splunk Documentation]

NEW QUESTION 72

When running the command shown below, what is the default path in which deployment server. conf is created?

splunk set deploy-poll deployServer:port
* SFLUNK_HOME/etc/deployment
* SPLUNK_HOME/etc/system/local
* SPLUNK_HOME/etc/system/default
* SPLUNK_KOME/etc/apps/deployment

NEW QUESTION 73

To set up a Network input in Splunk, what needs to be specified’?
* File path.
* Username and password
* Network protocol and port number.
* Network protocol and MAC address.

NEW QUESTION 74

What conf file needs to be edited to set up distributed search groups?
* props.conf
* search.conf
* distsearch.conf
* distibutedsearch.conf

Explanation/Reference: https://docs.splunk.com/Documentation/Splunk/8.0.5/DistSearch/Distributedsearchgroups

The SPLK-1003 exam covers a wide range of topics that are essential for Splunk administrators, including installation, configuration, data inputs, search and reporting, user management, and troubleshooting. Candidates must demonstrate a deep understanding of Splunk's architecture, components, and features, as well as its use cases and best practices. SPLK-1003 exam is designed to test both theoretical knowledge and practical skills, with a focus on real-world scenarios and challenges that administrators may encounter in their day-to-day work.

Get Instant Access to SPLK-1003 Practice Exam Questions: https://www.vceprep.com/SPLK-1003-latest-vce-prep.html]