Pass Your Exam With 100% Verified SPLK-1003 Exam Questions [Q10-Q24

Pass Your Exam With 100% Verified SPLK-1003 Exam Questions
SPLK-1003 Dumps PDF - SPLK-1003 Real Exam Questions Answers

Splunk SPLK-1003 certification exam is a valuable accreditation for professionals who are looking to gain expertise in Splunk Enterprise software. SPLK-1003 exam is designed for individuals who have experience in managing and deploying Splunk Enterprise environments. Splunk Enterprise Certified Admin certification is intended to demonstrate a candidate's proficiency in using Splunk Enterprise software to manage and analyze data.

Splunk Enterprise Certified Admin certification is an essential credential for professionals who work with Splunk Enterprise. It is an industry-recognized certification that demonstrates a candidate's ability to manage and maintain Splunk Enterprise environments effectively. Splunk Enterprise Certified Admin certification is highly valued by employers, and it can lead to better job opportunities and higher salaries. By passing the SPLK-1003 exam, candidates can prove their skills in Splunk administration and distinguish themselves from their peers in the IT industry.

NO.10 On the deployment server, administrators can map clients to server classes using client filters. Which of the following

statements is accurate?
* The blacklist takes precedence over the whitelist.
* The whitelist takes precedence over the blacklist.
* Wildcards are not supported in any client filters.
* Machine type filters are applied before the whitelist and blacklist.

NO.11 Which of the following is an appropriate description of a deployment server in a non-cluster environment?
* Allows management of local Splunk instances, requires Enterprise license, handles job of sending configurations packaged as apps. can automatically restart remote Splunk instances.
* Allows management of remote Splunk instances, requires Enterprise license, handles job of sending configurations, can automatically restart remote Splunk instances.
* Allows management of remote Splunk instances, requires no license, handles job of sending configurations, can automatically restart remote Splunk instances.
* Allows management of remote Splunk instances, requires Enterprise license, handles job of sending configurations, can manually restart remote Splunk instances.

NO.12 Which Splunk configuration file is used to enable data integrity checking?
* props.conf
* global.conf
* indexes.conf
* data_integrity.conf

NO.13 What is the correct order of steps in Duo Multifactor Authentication?
* 1 Request Login

2. Connect to SAML server

3 Duo MFA

4 Create User session

5 Authentication Granted 6. Log into Splunk
* 1. Request Login 2 Duo MFA

3. Authentication Granted 4 Connect to SAML server

5. Log into Splunk

6. Create User session
* 1 Request Login

2 Check authentication / group mapping

3 Authentication Granted

4. Duo MFA

5. Create User session

6. Log into Splunk

* 1 Request Login 2 Duo MFA

3. Check authentication / group mapping

4 Create User session

5. Authentication Granted

6 Log into Splunk
Explanation

Using the provided DUO/Splunk reference URL https://duo.com/docs/splunk 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.

NO.14 Which Splunk indexer operating system platform is supported when sending logs from a Windows universal forwarder?
* Any OS platform
* Linux platform only
* Windows platform only.
* None of the above.
Explanation

“The forwarder/indexer relationship can be considered platform agnostic (within the sphere of supported platforms) because they exchange their data handshake (and the data, if you wish) over TCP.

NO.15 Where are deployment server apps mapped to clients?
* Apps tab in forwarder management interface or clientapps.conf.
* Clients tab in forwarder management interface or deploymentclient.conf.
* Server Classes tab in forwarder management interface or serverclass.conf.
* Client Applications tab in forwarder management interface or clientapps.conf.
Explanation/Reference: https://docs.splunk.com/Documentation/Splunk/8.0.5/Updating/
Updateconfigurations#2._Reload_the_deployment_server

NO.16 After an Enterprise Trial license expires, it will automatically convert to a Free license. How many days is an Enterprise Trial license valid before this conversion occurs?
* 90 days
* 60 days
* 7 days
* 14 days

NO.17 Which valid bucket types are searchable? (Choose all that apply.)

* Hot buckets
* Cold buckets
* Warm buckets
* Frozen buckets

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

NO.18 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

NO.19 Which of the following are available input methods when adding a file input in Splunk Web? (Choose all that apply.)

* Index once.
* Monitor interval.
* On-demand monitor.
* Continuously monitor.

Explanation

https://docs.splunk.com/Documentation/Splunk/8.2.2/Data/Howdoyouwanttoadddata The fastest way to add data to your Splunk Cloud instance or Splunk Enterprise deployment is to use Splunk Web. After you access the Add Data page, choose one of three options for getting data into your Splunk platform deployment with Splunk Web: (1) Upload, (2) Monitor, (3) Forward The Upload option lets you upload a file or archive of files for indexing. When you choose Upload option, Splunk Web opens the upload process page. Monitor. For Splunk Enterprise installations, the Monitor option lets you monitor one or more files, directories, network streams, scripts, Event Logs (on Windows hosts only), performance metrics, or any other type of machine data that the Splunk Enterprise instance has access to.

NO.20 What action is required to enable forwarder management in Splunk Web?

* Navigate to Settings > Server Settings > General Settings, and set an App server port.
* Navigate to Settings > Forwarding and receiving, and click on Enable Forwarding.
* Create a server class and map it to a client in SPLUNK_HOME/etc/system/local/serverclass.conf.
* Place an app in the SPLUNK_HOME/etc/deployment-apps directory of the deployment server.

NO.21 Which of the following Splunk components require a separate installation package?

* Deployment server
* License master
* Universal forwarder
* Heavy forwarder

NO.22 What options are available when creating custom roles? (select all that apply)

* Restrict search terms
* Whitelist search terms
* Limit the number of concurrent search jobs
* Allow or restrict indexes that can be searched.

https://docs.splunk.com/Documentation/SplunkCloud/8.2.2106/Admin/ConcurrentLimits

“Set limits for concurrent scheduled searches. You must have the edit_search_concurrency_all and

edit_search_concurrency_scheduled capabilities to configure these settings.”

NO.23 A new forwarder has been installed with a manually createddeploymentclient.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 thephoneHomeIntervalInSecssetting.
Explanation

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.

References: Splunk Enterprise Certified Admin | Splunk, [Configure deployment clients – Splunk Documentation]

NO.24 An admin is running the latest version of Splunk with a 500 GB license. The current daily volume of new data is

300 GB per day. To minimize license issues, what is the best way to add 10 TB of historical data to the index?
* Buy a bigger Splunk license.
* Add 2.5 TB each day for the next 5 days.
* Add all 10 TB in a single 24 hour period.
* Add 200 GB of historical data each day for 50 days.

SPLK-1003 Dumps 100 Pass Guarantee With Latest Demo: https://www.vceprep.com/SPLK-1003-latest-vce-prep.html]