CERTKILLERS

Splunk

SPLK-1003 Exam

Splunk Enterprise Certified Admin

Thank you for Downloading SPLK-1003 exam PDF Demo

You can Buy Latest SPLK-1003 Full Version Download

https://www.certkillers.net/Exam/SPLK-1003

https://www.certkillers.net

Version: 16.2

Question: 1

Which setting in indexes. conf allows data retention to be controlled by time?

A. maxDaysToKeep
B. moveToFrozenAfter
C. maxDataRetentionTime
D. frozenTimePeriodlnSecs

Answer: D

Explanation:

https://docs.splunk.com/Documentation/Splunk/latest/Indexer/Setaretirementandarchivingpolicy

Question: 2

The universal forwarder has which capabilities when sending data? (select all that apply)

A. Sending alerts
B. Compressing data
C. Obfuscating/hiding data
D. Indexer acknowledgement

Answer: BD

Explanation:

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.

Question: 3

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:

https://docs.splunk.com/Documentation/Splunk/8.0.4/Data/Whitelistorblacklistspecificincomingdata

"It is not necessary to define both an allow list and a deny list in a configuration stanza. The settings are independent. If you do define both filters and a file matches them both, Splunk Enterprise does not index that file, as the blacklist filter overrides the whitelist filter." Source: https://docs.splunk.com/Documentation/Splunk/8.1.0/Data/Whitelistorblacklistspecificincomingdata

Question: 4

In which Splunk configuration is the SEDCMD used?

A. props, conf
B. inputs.conf
C. indexes.conf
D. transforms.conf

Answer: A

Explanation:

https://docs.splunk.com/Documentation/Splunk/8.0.5/Forwarding/Forwarddatatothird-partysystemsd
"You can specify a SEDCMD configuration in props.conf to address data that contains characters that the third-party server cannot process. "

Question: 5

Which of the following are supported configuration methods to add inputs on a forwarder? (select all that apply)

A. CLI
B. Edit inputs . conf
C. Edit forwarder.conf
D. Forwarder Management

Answer: ABD

Explanation:

https://docs.splunk.com/Documentation/Forwarder/8.2.1/Forwarder/HowtoforwarddatatoSplunkEn

terprise

"You can collect data on the universal forwarder using several methods. Define inputs on the universal forwarder with the CLI. You can use the CLI to define inputs on the universal forwarder. After you define the inputs, the universal forwarder collects data based on those definitions as long as it has access to the data that you want to monitor. Define inputs on the universal forwarder with configuration files. If the input you want to configure does not have a CLI argument for it, you can configure inputs with configuration files. Create an inputs.conf file in the directory, $SPLUNK_HOME/etc/system/local

`

Thank You for trying SPLK-1003 PDF Demo

To Buy New SPLK-1003 Full Version Download visit link below

https://www.certkillers.net/Exam/SPLK-1003

Start Your SPLK-1003 Preparation

Use Coupon "**CKNET**" for Further   discount on the purchase of Full Version Download. Test your SPLK-1003 preparation with actual exam questions.