SPLK-1003^{Q&As}

Splunk Enterprise Certified Admin

Pass Splunk SPLK-1003 Exam with 100% Guarantee

Free Download Real Questions & Answers **PDF** and **VCE** file from:

https://www.pass4itsure.com/splk-1003.html

100% Passing Guarantee
100% Money Back Assurance

Following Questions and Answers are all new published by Splunk
Official Exam Center

Instant Download After Purchase

100% Money Back Guarantee

365 Days Free Update

800,000+ Satisfied Customers

QUESTION 1

What is a role in Splunk? (select all that apply)

A. A classification that determines what capabilities a user has.

B. A classification that determines if a Splunk server can remotely control another Splunk server.

C. A classification that determines what functions a Splunk server controls.

D. A classification that determines what indexes a user can search.

Correct Answer: AD

A role in Splunk is a classification that determines what capabilities and indexes a user has.A capability is a permission to perform a specific action or access a specific feature on the Splunk platform1.An index is a collection of data that Splunk software processes and stores2. By assigning roles to users, you can control what they can do and what data they can access on the Splunk platform. Therefore, the correct answers are A and D. A role in Splunk determines what capabilities and indexes a user has. Option B is incorrect because Splunk servers do not use roles to remotely control each other.Option C is incorrect because Splunk servers use instances and components to determine what functions they control3. References:1:Define roles on the Splunk platform with capabilities - Splunk Documentation2:About indexes and indexers - Splunk Documentation3:Splunk Enterprise components - Splunk Documentation

QUESTION 2

How can native authentication be disabled in Splunk?

A. Remove the $SPLUNK_HOME/etc/passwd file

B. Create an empty $SPLUNK_HOME/etc/passwd file

C. Set SPLUNK_AUTHENTICATION=false in splunk-launch.conf

D. Set nativeAuthentication=false in authentication.conf

Correct Answer: B

Reference: https://docs.splunk.com/Documentation/Splunk/8.0.5/Security/Secureyouradminaccount

QUESTION 3

Which of the following methods will connect a deployment client to a deployment server? (select all that apply)

A. Run $SPLUNK_ROME/bin/ splunk set deploy-poll : from the command line of the deployment client.

B. Create and edit a deploymentserver . conf file in SSPLVNE{ on the deployment server.

C. Create and edit a deploymentclient . conf file in SSPLTJNE(EOME/etc/ system/local on the deployment client.

D. Run $SPLUNK ROME/bin/spiunk set deploy-poi i : from the command line of the deployment server.

Correct Answer: AC

The correct methods to connect a deployment client to a deployment server are A and C. You can either run the command splunk set deploy-poll : from the command line of the deployment client1 or create and edit a deploymentclient.conf file in $SPLUNK_HOME/etc/system/local on the deployment client2. Both methods require you to specify the IP address, hostname, and management port of the deployment server that you want the client to connect to.

QUESTION 4

After how many warnings within a rolling 30-day period will a license violation occur with an enforced Enterprise license?

A. 1

B. 3

C. 4

D. 5

Correct Answer: D

https://docs.splunk.com/Documentation/Splunk/8.0.5/Admin/Aboutlicenseviolations "Enterprise Trial license. If you get five or more warnings in a rolling 30 days period, you are in violation of your license. Dev/Test license. If you generate five or more warnings in a rolling 30-day period, you are in violation of your license. Developer license. If you generate five or more warnings in a rolling 30-day period, you are in violation of your license. BUT for Free license. If you get three or more warnings in a rolling 30 days period, you are in violation of your license."

Reference: https://docs.splunk.com/Documentation/Splunk/8.0.5/Admin/Aboutlicenseviolations

---

QUESTION 5

Which of the following are supported options when configuring optional network inputs?

A. Metadata override, sender filtering options, network input queues (quantum queues)

B. Metadata override, sender filtering options, network input queues (memory/persistent queues)

C. Filename override, sender filtering options, network output queues (memory/persistent queues)

D. Metadata override, receiver filtering options, network input queues (memory/persistent queues)

Correct Answer: B

https://docs.splunk.com/Documentation/Splunk/latest/Data/Monitornetworkports