Up-to-date Questions and Answers from authentic resources to improve knowledge and pass the exam at very first attempt. ----- Guaranteed.

KILL EXAMS

2B0-023 Dumps
2B0-023 Braindumps
2B0-023 Real Questions
2B0-023 Practice Test
2B0-023 Actual Questions

PASS

killexams.com

Enterasys

2B0-023

ES Advanced Dragon IDS

ORDER FULL VERSION

https://killexams.com/pass4sure/exam-detail/2B0-023

Console to work properly?

A. MySQL
B. DBI
C. Nessus
D. DataShowTable

Answer: C

QUESTION: 42
From where does Dragon Trending Console import event data?

A. Dragon Ring Buffer
B. Dragon DB Agent
C. Dragon Export Log Agent
D. Dragon Trending Console Agent

Answer: C

QUESTION: 43
Which Dragon configuration file allows you to modify Dragon Ring Buffer parameters?

A. /usr/dragon/dragon.cfg
B. /usr/dragon/tools/displayringstats
C. /usr/dragon/policymgr/driders.cfg
D. /usr/dragon/sensor/conf/dragon.net

Answer: A

QUESTION: 44
Given a scenario where an SSH session is already established between Host_A and Server_B, what is the effect on the established session if you PUSH a SNIPER ACL to a Network Sensor that is configured to block all SSH communication from Host_A?

A. The established session is immediately terminated, and all subsequent SSH attempts from Host_A are denied
B. The established session is immediately terminated, and all subsequent SSH attempts from Host_A are allowed
C. The established session remains active until the user terminates it, and all subsequent SSH attempts from Host_A are denied
D. Host Sensor immediately logs an event and initiates strong monitoring on Host_A, but allows all SSH to/from Host_A until an actual attack is detected

Answer: A

QUESTION: 45
What is the purpose of the rtu-mysql.pl script?

A. Tails the Dragon Export Log, parses the data, then imports the data into an SQL database
B. Starts the MySQL programs and connects the Dragon DB Agent to the Dragon Realtime Console Agent
C. Writes detected event data to a dragon.log file in ASCII format
D. Exports data from a MySQL database to a dragon.log file in ASCII format

Answer: A

QUESTION: 46
How can Dragon Workbench be configured to read a 'snoop' capture file on a Solaris host?

A. No configuration necessary; Workbench will read a 'snoop' file natively
B. Add the SNOOP keyword to the dragon.net file
C. Add a 'SNOOP=1' entry to the dragon.cfg file
D. Run the /usr/dragon/install/config script and select the Workbench snoop option

Answer: B

QUESTION: 47

Which of the following are true with regard to the catchTrap utility?

A. Will conflict with Host Sensor if run concurrently
B. Is located in the /usr/dragon/policymgr/tools directory
C. Monitors SNMP Traps during the phase of defining a Host Sensor SNMP-trap policy library
D. Provides SNMP alerting functionality for Dragon Alarmtool
E. Allows traps to be caught, parsed and displayed in much the same way that Host Sensor will process them
F. Analyzes traps and generates NIDS events for any anomalies within an SNMPv1 or SNMPv3 trap

Answer: A, C, E

QUESTION: 48
Which of the following are true with regard to Dragon Workbench?

A. Allows Dragon to replay data contained in TCPDUMP trace/capture files with the goal of tuning a Network Sensor prior to deployment
B. Can read data directly from the interface specified in the dragon.net file
C. Will create separate dragon.db files for each 24-hours worth of data contained in a TCPDUMP trace/capture file
D. Allows Dragon to compensate for the Snap Length limitation of TCPDUMP
E. Can read data from Snoop trace/capture files
F. Can analyze data contained in TCPDUMP trace/capture files and generate events based on anomalies

Answer: A, E, F

QUESTION: 49
What file must be present in the directory in which the 'reinstall' script is executed?

A. The dragon.cfg file
B. The config script
C. The Dragon software bundle in the .tar.gz format
D. The dragon.tar file after it has been extracted from the software bundle

Answer: D

QUESTION: 50
In UPN's 'Acceptable Use Policy', what proactive service is designed to complement a Dragon IDS deployment?

A. Deny Spoofing
B. Deny Unsupported Protocol Access
C. Protocol Priority Access Control
D. Dragon RealTime Console
E. Threat Management

Answer: E

SAMPLE QUESTIONS

*These questions are for demo purpose only. **Full version** is up to date and contains actual questions and answers.*

Killexams.com is an online platform that offers a wide range of services related to certification exam preparation. The platform provides actual questions, exam dumps, and practice tests to help individuals prepare for various certification exams with confidence. Here are some key features and services offered by Killexams.com:

***Actual Exam Questions**: Killexams.com provides actual exam questions that are experienced in test centers. These questions are updated regularly to ensure they are up-to-date and relevant to the latest exam syllabus. By studying these actual questions, candidates can familiarize themselves with the content and format of the real exam.*

***Exam Dumps**: Killexams.com offers exam dumps in PDF format. These dumps contain a comprehensive collection of questions and answers that cover the exam topics. By using these dumps, candidates can enhance their knowledge and improve their chances of success in the certification exam.*

***Practice Tests**: Killexams.com provides practice tests through their desktop VCE exam simulator and online test engine. These practice tests simulate the real exam environment and help candidates assess their readiness for the actual exam. The practice tests cover a wide range of questions and enable candidates to identify their strengths and weaknesses.*

***Guaranteed Success**: Killexams.com offers a success guarantee with their exam dumps. They claim that by using their materials, candidates will pass their exams on the first attempt or they will refund the purchase price. This guarantee provides assurance and confidence to individuals preparing for certification exams.*

***Updated Content:** Killexams.com regularly updates its question bank and exam dumps to ensure that they are current and reflect the latest changes in the exam syllabus. This helps candidates stay up-to-date with the exam content and increases their chances of success.*

***Technical Support**: Killexams.com provides free 24x7 technical support to assist candidates with any queries or issues they may encounter while using their services. Their certified experts are available to provide guidance and help candidates throughout their exam preparation journey.*