

TestInside Testing Engine Features

Comprehensive questions and answers about 2B0-101 exam

2B0-101 exam questions accompanied by exhibits

Verified Answers Researched by Industry Experts and almost 100% correct

2B0-101 exam questions updated on regular basis

Same type as the certification exams, 2B0-101 exam preparation is in multiple-choice questions (MCQs).

Tested by multiple times before publishing

Try free 2B0-101 exam demo before you decide to buy it in Test-Inside.com.

Note: This pdf demo do not include the question's picture.

Exam : Enterasys Networks 2B0-101

Title : Enterasys Security Systems Engineer (ESSE) Recertification

1. Dragonctl is used to?

- A. Start, stop and monitor the dragon processes on the remote node
- B. Write log files
- C. Monitor the Ring Buffer
- D. Maintain configuration channel connections

Answer: A

2. Which of the following best describes the commit operation?

- A. It uses the configuration channel to push a configuration to a device
- B. It uses the event channel to push a configuration to a device
- C. It writes a configuration change to the Enterprise Management Server (EMS) database
- D. It writes a configuration change to the management clients database

Answer: C

3. Which of the following Dragon Agents is used for detecting changes to host files?

- A. Real Time Console
- B. MD5 Sum
- C. Alarm Tool
- D. Database

Answer: B

4. The host policy MD5 detection module

- A. Detects any changes in the contents of protected file
- B. Detects file size increases
- C. Detects file truncations
- D. Detects ownership changes

Answer: A

5. Traffic direction refers to traffic flows in relation to the

- A. Server
- B. Protected network
- C. Client
- D. DMZ

Answer: B

6. Agents can be deployed?

- A. Only on non-forwarding Event Flow Processor (EFPs)
- B. Only on forwarding Event Flow Processor (EFPs)
- C. Only on the Enterprise Management Server (EMS) station
- D. On any Event Flow Processor (EFP)

Answer: D

7. Virtual Sensors can segregate traffic by?

- A. IP Address, VLAN, Port
- B. IP Address, VLAN, Port, Protocol
- C. IP Address, VLAN, Port, Protocol, Application
- D. IP Address, VLAN, Port, Application

Answer: B

8. The attack category is for events that

- A. Attempt to discover weaknesses
- B. Map the structure of the network
- C. Have the potential to compromise the integrity of an end system.
- D. Deny access to resources

Answer: C

9. Virtual sensor names?

- A. Are included in events they generate
- B. Must match the sensor key
- C. Must include the device name
- D. Require separate keys

Answer: A

10. If a packet matched the rules for two virtual sensors it will be evaluated by?

- A. Both sensors
- B. The first sensor it matches
- C. The default sensor
- D. Overlapping rules are not permitted

Answer: B

11. Agent status will show as Not Available until?

- A. The agent is committed
- B. The agent is deployed
- C. The agent is selected
- D. The remote node is deployed

Answer: B

12. Which alarm type is best described as: collects information for x period of time, then send event notifications

- A. Real Time
- B. Summary
- C. Dynamic
- D. Interval

Answer: B

13. Before the host Sensor can be deployed

- A. It must be associated with a virtual sensor
- B. It must be associated with a host policy
- C. Its key must be added to the /usr/dragon/bin directory
- D. Its address must be added to /etc/hosts

Answer: B

14. In an Event Flow Processor (EFP) a consumer can be?

- A. A Sensor or an Event Channel
- B. An Event channel only
- C. An Event channel or an Agent
- D. An Agent only

Answer: C

15. Which of the following Dragon Agents sends notifications when the sensors detect an event that match a rule?

- A. Real Time Console
- B. MD5 Sum
- C. Alarm Tool
- D. Database

Answer: C

16. Signature OS

- A. Applies signature to network traffic originating from the specified OS
- B. Is used for writing Host signatures
- C. Is optional on Network signatures
- D. Is required on all signatures

Answer: B

17. MD5 checksums are

- A. Stored in a protected directory on the host
- B. Appended to the protected file
- C. Passed up the event channel to the MD5 Agent
- D. Stored in the /usr/dragon/bin directory on the Enterprise Management Server (EMS)

Answer: C

18. In a standalone deployment the system will have?

- A. A net-config-client.xml file
- B. A net-config-server.xml file
- C. A net-config-server.xml and a net-con fig-client.xml file
- D. A net-config-server.xml, a net-con fig-client.xml and a net-config-reports.xml file

Answer: C

19. Agents can be deployed on?

- A. Only the Enterprise Management Server (EMS)
- B. Any managed node with a networked sensor deployed
- C. Any managed node with host sensor deployed
- D. Any managed node

Answer: D

20. The master Alarm Tool Default policy

- A. Is write locked
- B. Is writable
- C. Cannot be copied
- D. Cannot be associated with an Agent

Answer: A

[More 2B0-101 Information](#)

Related 2B0-101 Exams

[2B0-012](#) *ES Switching Edition 4.0*

[2B0-011](#) *ES Router Configuration*

[2B0-100](#) *Enterasys Systems Engineer (ESE) Recertification*

[2B0-021](#) *ES XSR Configuration*

[2B0-015](#) *ES Wireless*

[2B0-019](#) *ES Policy Enabled Networking*

[2B0-102](#) *Enterasys Security Systems Engineer-Defense*

[2B0-024](#) *ES Secure Networks*

[2B0-104](#) *Enterasys Certified Internetworking Engineer(ECIE)*

[2B0-101](#) *Enterasys Security Systems Engineer (ESSE) Recertification*

[2B0-020](#) *ES NetSight Atlas*

[2B0-022](#) *ES XSR Security*

[2B0-103](#) *Enterasys Security Systems Engineer-NAC*

[2B0-018](#) *ES Dragon IDS*

[2B0-023](#) *ES Advanced Dragon IDS*

Other Enterasys Networks Exams

[2B0-021](#)

[2B0-012](#)

[2B0-018](#)

[2B0-100](#)

[2B0-023](#)

[2B0-103](#)

[2B0-011](#)

[2B0-024](#)

[2B0-015](#)

[2B0-104](#)

[2B0-020](#)

[2B0-022](#)

[2B0-101](#)

[2B0-102](#)

[2B0-019](#)