



[Juniper Networks jn0-541](#)

Exam Name: IDP, Associate(JNCIA-IDP)

Q & A : 100 Q&As

Pdf Demo

Quality and Value for the jn0-541 Exam

[Just4Exams Practice Exams](#) for Juniper Networks JNCIA jn0-541 are written to the highest standards of technical accuracy, using only certified subject matter experts and published authors for development.

100% Guarantee to Pass Your jn0-541 Exam

If you do not pass the JNCIA jn0-541 exam on your first attempt using our Just4Exams *jn0-541 testing engine and pdf study guide*, we will give you a FULL REFUND of your purchasing fee.

Downloadable, Interactive jn0-541 Testing engines and PDF Version

Our Exam Preparation Material provides you everything you will need to take a [JNCIA certification](#) examination. Details are researched and produced by [Juniper Networks Certification](#) Experts who are constantly using industry experience to produce precise, and logical.

Free jn0-541 Exams:

This is demo only, this pdf do not include the questions and answers picture

Exam : Juniper JN0-541

Title : Juniper IDP, Associate(JNCIA-IDP)

1. Which interface does IDP use to communicate with Security Manager?

- A. eth0
- B. eth1
- C. HA port
- D. console port

Answer: A

2. Click the Exhibit button.

In the exhibit, which sensor command would have produced this display?

- A. sctop "t" option
- B. sctop "s" option
- C. scio policy list s0
- D. scio subs qmodules s0

Answer: A

3. You want Enterprise Security Profiler (ESP) to generate a message when a new host is detected on a network.

Which two steps must you perform? (Choose two.)

- A. Start or restart the profiler process.
- B. Configure ESP to enable alerts for new host detected.
- C. Configure ESP to enable application profiling, and select the contexts to profile.
- D. Under the Violation Viewer tab, create a permitted object, select that object, and then click Apply.

Answer: AB

4. Which type of cable do you use for a console connection to an IDP sensor?

- A. CAT 5 cable
- B. null-modem cable
- C. Juniper proprietary cable
- D. straight-through serial cable

Answer: B

5. Which TCP port is used for communication between ACM and an IDP sensor?

- A. 80
- B. 443
- C. 7800
- D. 7801

Answer: B

6. Which three are assigned as a result of running EasyConfig? (Choose three.)

- A. sensor default gateway
- B. sensor eth0 IP address
- C. sensor eth1 IP address
- D. sensor HA configuration
- E. sensor deployment mode

Answer: ABE

7. You implement Traffic Anomaly detection and you find numerous alerts of port scans from your security auditing team that you want to ignore. You create an address book entry for the security audit team specifying the IP addresses of those machines.

What should you do next?

- A. Create a rule at the top of the Traffic Anomaly rulebase to ignore traffic from security audit team.
- B. Create an exempt rule for the security audit team in the Exempt rulebase to ignore Traffic Anomalies.
- C. Create a rule at the top of the IDP rulebase to ignore traffic from security audit team, and make this a terminal rule.
- D. Create a rule at the top of the Traffic Anomaly rule base to ignore traffic from security audit team, and make this a terminal rule.

Answer: A

8. Given the following steps:

Which order is correct when initially deploying a sensor in a network?

- A. a, e, d, c, f, b
- B. e, a, d, b, f, c
- C. e, a, d, c, b, f
- D. b, f, e, a, d, c

Answer: B

9. In which three situations would you create a compound attack object? (Choose three.)

- A. When attack objects must occur in a particular order.
- B. When one of the attack objects is a protocol anomaly.
- C. You have at least two attack objects that define a single attack.
- D. When the pattern needs to be defined using a stream 256 context.
- E. When the pattern "@@#@#@#@#@#" and context "ftp-get-filename" completely define the attack.

Answer: ABC

10. What is "a deviation from a protocol's expected behavior or packet format"?

- A. context
- B. attack signature
- C. protocol anomaly
- D. compound attack object

Answer: C

11. Which three functions does the IDP sensor perform? (Choose three.)

- A. detects new hosts on the network
- B. displays logs in Security Manager GUI
- C. performs attack detection and prevention
- D. forwards logs and status messages to Security Manager server

Answer: ACD

12. Which three actions must be taken prior to deploying an IDP sensor (in transparent mode) in a network?

- A. Configure the sensor mode.
- B. Assign an IP to all forwarding interfaces.
- C. Assign an IP to the management interface IP.
- D. Establish communication between Security manager and the sensor.

Answer: ACD

13. Which OSI layer(s) of a packet does the IDP sensor examine?

- A. layers 2-4
- B. layers 2-7
- C. layers 4-7
- D. layer 7 only

Answer: B

14. Which three statements are true as they relate to a transparent mode IDP deployment? (Choose three.)

- A. Can actively prevent attacks on all traffic.
- B. An IP address must be defined on each forwarding interface.
- C. Can be installed in the network without changing IP addresses or routes.
- D. Uses paired ports, such that packets arriving on one port go out the other associated port.

Answer: ACD

15. Which two statements are true as they relate to a sniffer mode IDP sensor deployment? (Choose two.)

- A. An IP address must be assigned to the sniffer interface.
- B. It does not affect the performance or availability of the network.
- C. It provides passive monitoring only with limited attack prevention.
- D. IDP sensor cannot be managed by Security Manager in sniffer mode. IDP sensor cannot be managed by Security Manager in sniffer mode.

Answer: BC

16. When connecting to a sensor using SSH, which account do you use to login?

- A. root
- B. super
- C. admin
- D. netscreen

Answer: C

17. Which TCP port is used for communication between Security Manager and an IDP sensor?

- A. 443
- B. 7800
- C. 7801
- D. 7803

Answer: D

18. If the power is lost to an IDP sensor, which feature allows the traffic to continue to flow through the device?

- A. NIC bypass
- B. stateful inspection
- C. peer port modulation

D. protocol anomaly detection

Answer: A

19. A newly re-imaged sensor is running IDP 4.0 code. You want to assign IP address 10.1.1.1 to the sensor. Which method do you use to do this?

- A. Use SSH to connect to the sensor at IP 192.168.1.1. Login as root, and run ipconfig.
- B. Use SSH to connect to the sensor at IP 192.168.1.1. Login as admin, and run ipconfig.
- C. Connect to the sensor's console port, login as admin, and answer the EasyConfig questions.
- D. Connect to the sensor's console port, login as root, and answer the EasyConfig questions.

Answer: D

20. What is the default admin account password on the sensor?

- A. admin
- B. abc123
- C. juniper01
- D. password

Answer: B

More [jn0-541 Braindumps](#) Information

Related jn0-541 Exams

| | | | | |
|---------|---------|---------|---------|---------|
| JN0-100 | JN0-522 | JN0-342 | JN0-400 | JN0-141 |
| jn0-201 | jn0-320 | JN0-521 | JN0-341 | jn0-120 |
| JN0-311 | jn0-541 | jn0-570 | jn0-540 | JN0-562 |
| JN0-321 | jn0-561 | jn0-140 | jn0-520 | JN0-340 |

Other Juniper Networks Exams

| | | | | |
|---------|---------|---------|---------|---------|
| jn0-541 | jn0-530 | jn0-540 | jn0-201 | JN0-522 |
| JN0-100 | JN0-350 | JN0-331 | jn0-330 | JN0-532 |
| JN0-341 | JN0-400 | JN0-141 | JN0-342 | jn0-570 |
| jn0-130 | jn0-310 | JN0-340 | jn0-140 | jn0-531 |