

jn0-541 braindumps

Juniper Networks JNCIA

jn0-541: IDP, Associate(JNCIA-IDP)

Practice Exam: jn0-541 Exams

Exam Number/Code: jn0-541

Exam Name: IDP, Associate(JNCIA-IDP)

Questions and Answers: 100 Q&As

([JNCIA](#))



Exam : [jn0-541](#)

"IDP, Associate(JNCIA-IDP)", also known as jn0-541 exam, is a Juniper Networks certification. With the complete collection of exam questions, Just4Study has assembled to take you through 100 Q&As to your jn0-541 exam preparation. In the jn0-541 exam resources, you will cover every field and category in Juniper Networks Certification helping to ready you for your successful Juniper Networks Certification.

The exam questions cover the latest real test and with all the correct answer. we promise the Q&A for Juniper Networks JNCIA jn0-541 (IDP, Associate(JNCIA-IDP)) examination of original title complete coverage. jn0-541 exam questions help you pass the exam.

Just4Study jn0-541 Feature:

* High quality - High quality and valued for the jn0-541 Exam: 100% Guarantee to Pass Your jn0-541 exam and get your JNCIA certification.

* Authoritative - Authoritative braindumps with complete details about jn0-541 exam.

* Cheaper - Our Just4Study products are cheaper than any other website. With our completed JNCIA resources, you will minimize your **Juniper Networks JNCIA** cost and be ready to pass your jn0-541 exam on Your First Try, 100% Money Back Guarantee included!

* Free - Try free JNCIA demo before you decide to buy it in <http://www.Just4Study.com>.

Just4Study Guarantee:

Just4Study provides the most competitive quality of all exams for the customers, we guarantee your success at the first attempt with only our Certification Question&Answers, if you do not pass the jn0-541 exam at the first time, we will not only arrange FULL REFUND for you, but also provide you another exam of your claim, ABSOLUTELY FREE!

Free jn0-541 Demo Download

Just4Study offers free demo for JNCIA jn0-541 exam (IDP, Associate(JNCIA-IDP)). You can check out the interface, question quality and usability of our practice exams before you decide to buy it. We are the only one site can offer demo for almost all products.

The Questions & Answers cover the latest real test and with all the correct answer.we promise the Q&A for **Juniper Networks JNCIA jn0-541** examination of original title complete coverage.jn0-541 Questions & Answers help you pass the exam. Otherwise,we will give you a full refund.

VUE/Prometric Code: jn0-541

Exam Name: IDP, Associate(JNCIA-IDP)([JNCIA](#))

Questions and Answers: 100 Q&A

[Juniper Networks jn0-541](#) Test belongs to one of the JNCIA certified test, if needs to obtain the JNCIA certificate, you also need to participate in other related test, the details you may visit the [JNCIA](#) certified topic, in there, you will see all related JNCIA certified subject of examination.

Just4Study professional provide JNCIA jn0-541 the newest Q&A, completely covers jn0-541 test original topic. With our complete JNCIA resources, you will minimize your JNCIA cost and be ready to pass your jn0-541 tests on Your First Try, 100% Money Back Guarantee included!

Just4Study Help You Pass Any IT Exam

[Just4Study.com](#) offers incredible career enhancing opportunities. We are a team of IT professionals that focus on providing our customers with the most up to date material for any IT certification exam. This material is so effective that we Guarantee you will pass the exam or your money back.

Exam : Juniper JN0-541

Title : Juniper IDP, Associate(JNCIA-IDP)

1. 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

2. 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

3. 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

4. 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

5. 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

6. 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

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

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

Answer: C

8. 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

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

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

Answer: D

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

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

Answer: B

11. 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

12. 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

13. 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

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

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

Answer: B

15. 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

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

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

Answer: A

17. 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

18. 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

19. 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

20. 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

[jn0-541 Braindumps](#)

Related jn0-541 Exams

[JN0-100](#) Juniper Networks Certified Internet Associate (JNCIA-JUNOS)

[JN0-522](#) Juniper Networks Certified Internet Associate, FWV (JNCIA-FWV)

[JN0-400](#) EX, Associate (JNCIA-EX)

[JN0-342](#) ER, Associate(JNCIA-ER)

[JN0-141](#) Juniper Networks Certified Internet Associate, AC (JNCIA-AC)

[jn0-201](#) juniper networks certified internet associate.m(jncia-m)

[jn0-320](#) Juniper Networks Certified Juniper DX (DXAP) Associate Exam

[JN0-521](#) FWV.Associate (JNCIA-FWV)

[JN0-341](#) ER.Associate(JNCIA-ER)

[JN0-311](#) WX, Associate(JNCIA-WX)

[jn0-120](#) juniper networks certified internet associate.e(jncia-e)

[jn0-541](#) IDP, Associate(JNCIA-IDP)

[jn0-570](#) JN0-570 JNCIS-SSL EXAM

[jn0-540](#) juniper networks certified internet associate.idp(jncia-idp)

[jn0-140](#) Certified Internet Associate (JNCIA-AC) 140 Exam

[jn0-561](#) Juniper Networks Certified Internet Assoc(JNCIA-SSL) Exam

[jn0-520](#) juniper networks certified internet associate(jncia-fwv)

[JN0-321](#) DX, Associate(JNCIA-DX)

[JN0-562](#) Certified Internet Associate (JNCIA-SSL) 562 Exam

[jn0-310](#) Juniper Networks Certified Internet Associate, WX (JNCIA-WX)

Other Juniper Networks Exams

[jn0-530](#) [jn0-541](#) [JN0-340](#) [JN0-562](#) [JN0-350](#) [JN0-331](#) [jn0-120](#) [jn0-320](#)

[JN0-400](#) [JN0-321](#) [jn0-520](#) [jn0-570](#) [jn0-130](#) [JN0-521](#) [jn0-201](#) [jn0-303](#)

[jn0-310](#) [jn0-561](#) [JN0-311](#) [JN0-522](#)