JN0-541

Juniper

IDP.Associate (JNCIA-IDP)

OfficialCerts.com is a reputable IT certification examination guide, study guides and audio exam provider. We ensure that you pass your JN0-541 exam in first attempt and also get high scores to acquire Juniper certification.

If you use OfficialCerts JN0-541 Certification questions and answers, you will experience actual JN0-541 exam questions/answers. We know exactly what is needed and have all the exam preparation material required to pass the exam. Our Juniper exam prep covers over 95% of the questions and answers that may be appeared in your JN0-541 exam. Every point from pass4sure JN0-541 PDF, JN0-541 review will help you take Juniper JN0-541 exam much easier and become Juniper certified.

Here's what you can expect from the OfficialCerts Juniper JN0-541 course:

** Up-to-Date Juniper JN0-541 questions as experienced in the real exam.*
** 100% correct Juniper JN0-541 answers you simply can't find in other JN0-541 courses.*
** All of our tests are easy to download. Your file will be saved as a JN0-541 PDF.*
** Juniper JN0-541 brain dump free content featuring the real JN0-541 test questions.*

Juniper JN0-541 certification exam is of core importance both in your Professional life and Juniper certification path. With Juniper certification you can get a good job easily in the market and get on your path for success. Professionals who passed Juniper JN0-541 exam training are an absolute favorite in the industry. You will pass Juniper JN0-541 certification test and career opportunities will be open for you.

http://www.officialcerts.com/exams.asp?examcode=JN0-541

JN0-541

QUESTION 1
Which statement is true about the attack object database update process?

A. Each sensor updates its own attack object database automatically; however they must be able to access the Juniper site on TCP port 443.
B. The attack object database update must be manually performed by the administrator, and the administrator must manually install it on each sensor.
C. The attack object database update can be initiated manually or automatically.
D. The attack object database update can be automatically scheduled to occur using the Security Manager GUI.

Answer: C

QUESTION 2
On a sensor, which command will indicate if log messages are being sent to Security Manager?

A. scio vr list
B. service idp status
C. scio agentstats display
D. scio getsystem

Answer: C

QUESTION 3
After you enable alerts for new hosts that are detected by the Enterprise Security Profiler, where do you look in Security Manager to see those alerts?

A. Security Monitor > Profiler > Application Profiler tab
B. Security Monitor > Profiler > Violation Viewer tab
C. Security Monitor > Profiler > Network Profiler tab
D. Log Viewer > Profiler Log

Answer: D

QUESTION 4
When connecting to a sensor using SSH, which account do you use to login?

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

Answer: A

QUESTION 5
Which OSI layer(s) of a packet does the IDP sensor examine?

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

Answer: A

QUESTION 6
Which two will change the management IP of an IDP sensor? (Choose two.)

A. Edit the existing IDP sensor object in Security Manager GUI and change the IP address.
B. Delete the IDP sensor object from Security Manager and re-add the sensor with the new IP address.
C. Use ifconfig to change the management IP address.
D. Use the ACM to change the management IP address.

Answer: B,D

QUESTION 7
Which rule base would detect netcat?

A. SYN protector
B. traffic anomalies
C. backdoor
D. exempt

Answer: C

QUESTION 8
Which three fields in a packet must match an IDP rule before that packet is examined for an attack? (Choose three.)

A. terminate match
B. service
C. destination address
D. source address
E. attack object

Answer: B,C,D

QUESTION 9
What is "a deviation from a protocol's expected behavior or packet format"?

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

Answer: D

QUESTION 10
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. Connect to the sensor's console port, login as root, and answer the EasyConfig questions.
B. Use SSH to connect to the sensor at IP 192.168.1.1. Login as root, and run ipconfig.
C. Connect to the sensor's console port, login as admin, and answer the EasyConfig questions.
D. Use SSH to connect to the sensor at IP 192.168.1.1. Login as admin, and run ipconfig.

Answer: A

QUESTION 11
Which rule base would detect the use of nmap on a network?

A. SYN protector
B. traffic anomalies
C. backdoor
D. exempt

Answer: B

QUESTION 12
Which type of cable do you use for a console connection to an IDP sensor?

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

Answer: D

QUESTION 13
Which statement is true regarding IDP rule matching on a sensor?

A. Each rule in the IDP rule base that matches on the source IP, destination IP, and service will be processed further.

PASS4SURE Officialcerts.com

OfficialCerts.com Certification Exam Full Version Features;

- Verified answers researched by industry experts.
- Exams **updated** on regular basis.
- Questions, Answers are downloadable in **PDF** format.
- **No authorization** code required to open exam.
- **Portable** anywhere.
- 100% success ***Guarantee***.
- **Fast**, helpful support 24x7.

View list of All exams we offer;
http://www.officialcerts.com/allexams.asp

To contact our Support;
http://www.officialcerts.com/support.asp

View FAQs
http://www.officialcerts.com/faq.asp

Download All Exams Samples
http://www.officialcerts.com/samples.asp

To purchase Full Version and updated exam;
http://www.officialcerts.com/allexams.asp

Shop now using PayPal

3COM	CompTIA	Filemaker	IBM	LPI	OMG	Sun
ADOBE	ComputerAssociates	Fortinet	IISFA	McAfee	Oracle	Sybase
APC	CWNP	Foundry	Intel	McData	PMI	Symantec
Apple	DELL	Fujitsu	ISACA	Microsoft	Polycom	TeraData
BEA	ECCouncil	GuidanceSoftware	ISC2	Mile2	RedHat	TIA
BICSI	EMC	HDI	ISEB	NetworkAppliance	Sair	Tibco
CheckPoint	Enterasys	Hitachi	ISM	Network-General	SASInstitute	TruSecure
Cisco	ExamExpress	HP	Juniper	Nokia	SCP	Veritas
Citrix	Exin	Huawei	Legato	Nortel	See-Beyond	Vmware
CIW	ExtremeNetworks	Hyperion	Lotus	Novell	Google	