



# JN0-541<sup>Q&As</sup>

IDP, Associate(JNCIA-IDP)

## Pass Juniper JN0-541 Exam with 100% Guarantee

Free Download Real Questions & Answers **PDF** and **VCE** file from:

<https://www.geekcert.com/jn0-541.html>

100% Passing Guarantee  
100% Money Back Assurance

Following Questions and Answers are all new published by Juniper  
Official Exam Center

- ⚙ **Instant Download** After Purchase
- ⚙ **100% Money Back** Guarantee
- ⚙ **365 Days** Free Update
- ⚙ **800,000+** Satisfied Customers





## QUESTION 1

When Address Resolution is enabled in the Log Viewer, which machine is responsible for performing the DNS Lookups?

- A. IDP Sensor
- B. WHOIS Servers
- C. IDP User Interface
- D. IDP Management Server

Correct Answer: B

flag	alarm	time received	attack	action	source address	src port	destination address	dst port
		3/15/06 6:59:09 AM	Spyware: 123Mania	drp packet	ZERO-ONE	3206	64.34.169.61	http
		3/15/06 6:59:18 AM	Spyware: 123Mania	drp packet	ZERO-ONE	0	64.34.169.61	http
		3/15/06 6:59:23 AM	Spyware: 123Mania	drp packet	ZERO-ONE	3221	64.34.169.61	http
		3/15/06 6:59:32 AM	Spyware: 123Mania	drp packet	ZERO-ONE	0	64.34.169.61	http
		3/15/06 6:59:57 AM	Spyware: 123Mania	drp packet	ZERO-ONE	3236	64.34.169.61	http
		3/15/06 7:00:06 AM	Spyware: 123Mania	drp packet	ZERO-ONE	0	64.34.169.61	http
		3/15/06 7:00:13 AM	Spyware: 123Mania	drp packet	ZERO-ONE	3252	64.34.169.61	http
		3/15/06 7:00:22 AM	Spyware: 123Mania	drp packet	ZERO-ONE	0	64.34.169.61	http
		3/15/06 7:01:04 AM	Spyware: 123Mania	drp packet	ZERO-ONE	3294	64.34.169.61	http
		3/15/06 7:01:14 AM	Spyware: 123Mania	drp packet	ZERO-ONE	0	64.34.169.61	http
		3/15/06 7:01:18 AM	Spyware: 123Mania	drp packet	ZERO-ONE	3315	64.34.169.61	http
		3/15/06 7:01:28 AM	Spyware: 123Mania	drp packet	ZERO-ONE	0	64.34.169.61	http
		3/15/06 11:52:49 AM	Spyware: ExactSearch	drp packet	Bluecoat Proxy SG	18005	tm.wc.ask.com	http
		3/15/06 11:52:57 AM	Spyware: ExactSearch	drp packet	Bluecoat Proxy SG	0	0.0.0.0	http
		3/15/06 11:53:21 AM	Spyware: ExactSearch	drp packet	Bluecoat Proxy SG	18031	cm.wc.ask.com	http
		3/15/06 11:53:42 AM	Spyware: ExactSearch	drp packet	Bluecoat Proxy SG	18042	cm.wc.ask.com	http
		3/15/06 11:55:48 AM	Spyware: ExactSearch	drp packet	Bluecoat Proxy SG	18094	cm.wc.ask.com	http
		3/15/06 11:55:57 AM	Spyware: ExactSearch	drp packet	Bluecoat Proxy SG	0	0.0.0.0	http
		3/15/06 11:56:21 AM	Spyware: ExactSearch	drp packet	Bluecoat Proxy SG	18104	cm.wc.ask.com	http
		3/15/06 11:56:42 AM	Spyware: ExactSearch	drp packet	Bluecoat Proxy SG	18106	cm.wc.ask.com	http
		3/15/06 8:35:06 PM	Spyware: CrackSpider	drp packet	Bluecoat Proxy SG	28091	213.244.183.199	http
		3/15/06 8:38:06 PM	Spyware: CrackSpider	drp packet	Bluecoat Proxy SG	28421	213.244.183.199	http
		3/15/06 11:16:03 PM	Spyware: CrackSpider	drp packet	Bluecoat Proxy SG	35746	213.244.183.199	http
		3/15/06 11:19:02 PM	Spyware: CrackSpider	drp packet	Bluecoat Proxy SG	35918	213.244.183.199	http

SummaryAll FieldsWhois LookupProfile Information

Query192.187.224.228Whois Serverwhois.arin.net

OrgName: ICG NetAhead, Inc.  
OrgID: ICGM  
Address: 161 Inverness Drive West  
City: Englewood  
StateProv: CO

## QUESTION 2

What should you do to purge logs for certain days from your IDP Management Server?

- A. purge the logs from the IDP User Interface



- B. Logs cannot be purged until the disk is full.
- C. Purge the logs manually from the CLI of each IDP Sensor
- D. Purge the logs manually from the CLI of the IDP Management Server

Correct Answer: A

---

### QUESTION 3

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

Correct Answer: D

---

### QUESTION 4

When creating a new signature-based attack object, which four components must be specified? (Choose four.)

- A. target platform
- B. IP header values
- C. time binding
- D. service binding
- E. context
- F. attack pattern

Correct Answer: ADEF

---

### QUESTION 5

Which account do you use to login when connecting to a sensor using SSL?

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



Correct Answer: D

[Latest JN0-541 Dumps](#)

[JN0-541 VCE Dumps](#)

[JN0-541 Braindumps](#)