

250-501 braindumps

Symantec Symantec Certified Security program

250-501: intrusion protection solutions

Practice Exam: 250-501 Exams

Exam Number/Code: 250-501

Exam Name: intrusion protection solutions

Questions and Answers: 140 Q&As

([Symantec Certified Security program](#))



"intrusion protection solutions", also known as 250-501 exam, is a Symantec certification. With the complete collection of exam questions, Just4Study has assembled to take you through 140 Q&As to your 250-501 exam preparation. In the 250-501 exam resources, you will cover every field and category in Symantec Certification helping to ready you for your successful Symantec Certification.

Exam : [250-501](#)

The exam questions cover the latest real test and with all the correct answer. we promise the Q&A for Symantec Symantec Certified Security program 250-501 (intrusion protection solutions) examination of original title complete coverage. 250-501 exam questions help you pass the exam.

Just4Study 250-501 Feature:

* High quality - High quality and valued for the 250-501 Exam: 100% Guarantee to Pass Your 250-501 exam and get your Symantec Certified Security program certification.

* Authoritative - Authoritative braindumps with complete details about 250-501 exam.

* Cheaper - Our Just4Study products are cheaper than any other website. With our completed Symantec Certified Security program resources, you will minimize your **Symantec Symantec Certified Security program** cost and be ready to pass your 250-501 exam on Your First Try, 100% Money Back Guarantee included!

* Free - Try free Symantec Certified Security program 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 250-501 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 250-501 Demo Download

Just4Study offers free demo for Symantec Certified Security program 250-501 exam (intrusion protection solutions). 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 **Symantec Symantec Certified Security program 250-501** examination of original title complete coverage. 250-501 Questions & Answers help you pass the exam. Otherwise, we will give you a full refund.

VUE/Prometric Code: 250-501

Exam Name: intrusion protection solutions(Symantec Certified Security program)

Questions and Answers: 140 Q&A

[Symantec 250-501](#) Test belongs to one of the Symantec Certified Security program certified test, if needs to obtain the Symantec Certified Security program certificate, you also need to participate in other related test, the details you may visit the [Symantec Certified Security program](#) certified topic, in there, you will see all related Symantec Certified Security program certified subject of examination.

Just4Study professional provide Symantec Certified Security program 250-501 the newest Q&A, completely covers 250-501 test original topic. With our complete Symantec Certified Security program resources, you will minimize your Symantec Certified Security program cost and be ready to pass your 250-501 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 : Symantec 250-501

Title : Intrusion Protection Solutions

1. Which service is required to deploy a Symantec Enterprise Security Architecture Manager?

- A. IBM HTTP Server
- B. iPlanet Web Server
- C. Netscape Web Server
- D. Internet Information Server

Answer: A

2. Which solution provides a robust management and reporting framework for Symantec Host IDS?

- A. Symantec Security Management System
- B. Symantec Host IDS Manager and Agent Tools
- C. Symantec Intrusion Protection Enterprise Manager
- D. Symantec Enterprise Security Management Console

Answer: A

3. Which two methods might you use to create custom policies? (Choose two.)

- A. build from scratch
- B. use the policy template
- C. import system registry settings
- D. export and modify a stock policy

Answer: AD

4. To which mode must you set the network interface on a network intrusion detection sensor to collect all packets?

- A. report
- B. receive
- C. transfer
- D. promiscuous

Answer: D

5. Which three types of network traffic should be considered suspicious by a deception-based intrusion system running on your corporate Intranet? (Choose three.)

- A. FTP connection
- B. broadcast traffic
- C. HTTP get request

D. SSL logon attempt

Answer: ACD

6. What is a possible risk of operating a decoy-based intrusion detection system on your network?

- A. Attackers could use the decoy to compromise another system making you liable.
- B. Attackers learn how to circumvent your perimeter defense through the decoy.
- C. The decoy reduces network performance by generating broadcast traffic on the network.
- D. The decoy may give away information about your network and other legitimate systems

Answer: A

7. Click the Exhibit button. What is the minimum number of Symantec Security Management System Console computers required to monitor the Boston office locally, while managing the entire Symantec Host IDS deployment from New York?

- A. 1
- B. 2
- C. 4
- D. 15

Answer: B

8. Which statement is true regarding Symantec Host IDS policy behavior?

- A. Policies are collected from Symantec Host IDS Agent computers.
- B. Policies are distributed to all Symantec Host IDS Agent computers.
- C. Policies are based on application settings on all computers running Symantec Host IDS.
- D. Policies are monitored on all computers running Symantec Host IDS Manager services.

Answer: B

9. Which activity compromises the integrity of forensic data collected during an incident response investigation of HostA?

- A. modification of firewall settings to collect additional forensic data
- B. modification of the system files on HostA to block further intrusions
- C. modification of the network intrusion detection system's signature files
- D. modification of the intrusion policy at HostA's IPS sensor to block further intrusions

Answer: B

10. Which two conditions affect the performance of network-based intrusion detection systems? (Choose two.)

- A. local area network traffic congestion
- B. resource utilization on sensor nodes
- C. presence of a host-based intrusion detection system
- D. concurrent support for intrusion detection across multiple platforms

Answer: AB

11. Which two types of policies are supported by Symantec Host IDS? (Choose two.)

- A. stock
- B. update
- C. custom
- D. best practice

Answer: AC

12. Which two technologies act as intrusion protection sensors? (Choose two.)

- A. routers
- B. host agents
- C. deception hosts
- D. managed switches

Answer: BC

13. Which service facilitates the automatic update of Symantec Host IDS stock policies?

- A. Symantec LiveUpdate
- B. Symantec PolicyEditor
- C. Symantec PolicyUpdate
- D. Symantec Host IDSUpdate

Answer: A

14. Which two states are monitored by statistical anomaly filters to detect changes in network activity? (Choose two.)

- A. protocol traffic rates
- B. changes in file sizes
- C. user account misuse
- D. users' activity over the network

Answer: AD

15. Which type of device is associated with passive intrusion detection strategies?

- A. firewall
- B. packet filter
- C. network sniffer
- D. management console

Answer: C

16. Which three organizations actively monitor the release of patches and upgrades from vendors? (Choose three.)

- A. CERT
- B. Microsoft
- C. Symantec
- D. Security Focus
- E. Sun Microsystems

Answer: ACD

17. Where are Symantec Host IDS events recorded?

- A. the DataStore
- B. the Directory
- C. the Local Agent log
- D. the Symantec Host IDS Manager

Answer: A

18. Which type of attacks are anomaly-based intrusion detection systems primarily designed to detect?

- A. novel
- B. known
- C. host-based
- D. network-based

Answer: A

19. Which Symantec Security Management System view displays Symantec Host IDS events?

- A. Symantec Host IDS Events folder, Intrusion Detection Events view
- B. Symantec Host IDS Events folder, Intrusion Detection Attack view
- C. Intrusion Detection Family folder, Symantec Host IDS Events view
- D. Intrusion Detection Reports folder, Symantec Host IDS Attack view

Answer: C

20. What is a characteristic unique to a host-based intrusion protection solution?

- A. service specific
- B. protocol specific
- C. topology specific
- D. operating system specific

Answer: D

[250-501 Braindumps](#)

Related 250-501 Exams

250-308	<i>Administration of Symantec Enterprise Vault 8.0 for Exchange</i>
250-311	<i>Admin of Symantec Endpoint Protection 11.0 for Windows</i>
250-312	<i>Administration of Symantec Backup Exec 12 fo Windows Server</i>
250-265	<i>Data Protection Administration for UNIX using NetBackup 6.5</i>
250-250	<i>Veritas Storage Foundation 5.0 Administration for UNIX</i>
250-351	<i>Administration of HA Solutions for Windows using VCS 5.0</i>
250-365	<i>Data Protection Administration for Windows(NBU 6.5)</i>
251-365	<i>Data Protection Administration for Windos(NBU 6.5)</i>
250-251	<i>Administration of HA Solutions for UNIX (VCS 5.0)</i>
251-250	<i>Administration of Staorage Foundation 5.0 for UNIX</i>
251-265	<i>Data Protection Administration for UNIX(NBU 6.5)</i>
250-223	<i>Data Protection Administration for UNIX using NBU 5.0</i>
250-240	<i>Administration of Storage Foundation 4.0 for UNIX</i>
250-824	<i>Data Protection Troubleshooting for UNIX using NetBackup 5.x</i>
250-323	<i>Data Protection Administration for Windows using NBU 5.0</i>
250-300	<i>Administration of Backup Exec 10 for Windows</i>
250-622	<i>Implementation of DP Solutions for UNIX using NBU 5.0</i>
250-422	<i>Design & Custom. of HA Solutions for UNIX using VCS 4.1</i>
251-251	<i>Administration of HA Solutions for UNIX(VCS 5.0)</i>
250-521	<i>Design of DP Solutions for Windows using NBU 5.0</i>

Other Symantec Exams

250-222	251-312	250-422	250-522	250-700	250-101	250-311	250-312
251-365	250-501	250-503	250-251	250-421	250-300	250-223	250-308
250-521	250-250	251-265	250-722				